Cyber Attacks, Attribution, and Deterrence: Three Case Studies

A Monograph

by

MAJ William Detlefsen

United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2015-01

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
23-05-2015	Master's Thesis	JUN 2014 – MAY 2015

4. TITLE AND SUBTITLE
Cyber attacks, Attribution, and Deterrence: Three Case Studies

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ William R. Detlefsen

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Advanced Operational Arts Studies Fellowship, Advanced Military Studies Program

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
What are the effects of delayed or denied attribution on deterring cyber attacks? Because of the speed at which cyber attacks can occur, it is important to understand how countries using cyber weapons frame the problem. The paper examined three cyber attacks: the 2007 attacks on Estonia, Stuxnet, and LulzSec's attacks on multiple targets in 2011. The defenders could not immediately attribute the attack to an actor, influencing how they responded to the problem.

However, attribution was not the defenders' biggest problem in two of the cases. Attribution may not always be immediately available, but eventually defenders had enough information on which to act. Other problems arose, like escalating a conflict with a more powerful neighbor or determining how to respond without a cyber capability of one's own. These cases demonstrate attribution is a necessary but not sufficient cause for responding and that defenders have many options available, from technical defense of their networks to escalation into conventional military strikes. Cyber deterrence does not require high levels of attribution because the target is typically a known adversary and the results from a cyber attack are generally much lower than the effects from conventional attacks. Because a state must be able to respond to cyber attacks in kind and the lower attribution requirements, an offensive cyber capability is both necessary and useful.

15. SUBJECT TERMS
Cyber, attribution, deterrence, Estonia, Stuxnet, LulzSec

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			MAJ William Detlefsen
(U)	(U)	(U)	(U)	53	**19b. PHONE NUMBER** *(include area code)*

Monograph Approval Page

Name of Candidate: MAJ William Detlefsen

Monograph Title: Cyber Attacks, Attribution, and Deterrence: Three Case Studies

Approved by:

_____, Monograph Director
Michael Mihalka, PhD

_____, Seminar Leader
Michael Rayburn, COL

_____, Director, School of Advanced Military Studies
Henry A. Arnold III, COL

Accepted this 23rd day of May 2015 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, PhD

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the US Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

Abstract

Monograph Title: Cyber Attacks, Attribution, and Deterrence: Three Case Studies, by MAJ William Detlefsen, 53 pages.

The purpose of this monograph is to examine the role of a defender's ability to attribute a cyber attack and its effect on deterrence. Conflict in cyberspace is constantly evolving and deterrence might provide stability and understanding of these conflicts. Because of the speed at which cyber attacks can occur and the rate at which they can spread, it is important to understand how countries using cyber weapons frame the problem.

The method used in this paper is controlled comparison of three different cyber attacks: the 2007 attacks on Estonia, the Stuxnet attack on Iran, and the LulzSec attacks multiple targets in 2011. These three events bore the similarity that defenders could not immediately attribute the attack to an actor. This attribution problem influenced how the defenders responded to the problem.

Upon further research, however, it became apparent that attribution was not the defenders' biggest problem in two of the three cases. Attribution may not always be immediately available through technical means, but eventually defenders had enough information on which to act. At this point, other problems arose, like escalating a cyber conflict with a far more powerful neighbor or determining how to respond without a cyber capability of one's own. These cases demonstrate attribution is a necessary but not sufficient cause for responding to a cyber attack and that defenders have many response options available, from technical defense of their networks to escalation of the conflict to kinetic military strikes.

Additionally, cyber deterrence does not require the high levels of attribution that some theorists argue. Instead, a counterattack can rely on a lower level of attribution because the target is typically a known adversary and because the results from a cyber attack are generally much lower than the effects from a kinetic attack. Thus, because of the need for a state to respond to cyber attacks in kind and the lower attribution requirements, an offensive cyber capability is both necessary and useful.

Contents

Acknowledgments

I would like to thank my monograph director, Dr. Michael Mihalka, for his assistance and guidance in writing this monograph and my seminar leader, COL Michael Rayburn, for his mentorship over the course of my time at the School of Advanced Military Studies (SAMS). I also wish to extend my gratitude to the leadership of the Indiana National Guard who took the chance on sending me to SAMS and my coworkers for picking up my share of the work so I could attend. Lastly, I must thank my wife and children for bearing my absence while I was gone.

Acronyms

CERT	Computer Emergency Response Team
DDoS	Distributed Denial of Service
FBI	Federal Bureau of Investigation
IP	Internet Protocol
PBS	Public Broadcasting Service
SCADA	Supervisory Control and Data Acquisition

Illustrations

Figures

Tables

Introduction

> America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas.[1]
>
> - Barack Obama, President of the United States of America

President Obama has said the United States of America must treat its digital infrastructure as a national security asset.[2] The Chairwoman of the US Senate Intelligence Committee stated, "Cyber attacks present the greatest threat to our national and economic security today, and the magnitude of the threat is growing."[3] And the Department of Defense has said "cyber capabilities have become integrated into our daily lives and have become vital to US national security."[4] Yet the recent theft of emails, movies, and proprietary data from Sony by a group calling itself the "Guardians of Peace" illustrates the continuing difficulty in preventing cyber attacks.[5]

---

[1] "Cybersecurity," The White House, accessed December 7, 2014, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

[2] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House, May 29, 2009, accessed September 25, 2014, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[3] Alina Selyukh and Patricia Zengerle. "Senate Intelligence Committee Approves Cybersecurity Bill," July 8, 2014, accessed October 2, 2014, http://www.reuters.com/article/2014/07/08/us-usa-cybersecurity-congress-idUSKBN0FD2LG20140708.

[4] "Deputy Assistant Secretary of Defense for Cyber Policy," US Department of Defense, accessed October 2 2014, 2014, http://policy.defense.gov/OUSDPOffices/ASDforHomelandDefenseGlobalSecurity/CyberPolicy.aspx.

[5] Zetter, Kim. "Sony Hackers Threaten to Release a Huge 'Christmas Gift' of Secrets.'" Wired. December 15, 2014. Accessed February 3, 2015. http://www.wired.com/2014/12/sony-hack-part-deux/.

The expansion of the internet and the proliferation of devices connected to it means more people have access to the internet, for good or ill. The internet is responsible for twenty per cent of the economic growth in mature countries and represents three per cent of the Gross Domestic Product, so the cyberspace has become the ocean for shopping, finance, and information for the twenty-first century.[6] As empires fought to control the seas, so too will they fight on the internet. Similarly, pirate-like actors occupy the blank spots on the map of cyberspace and work both for their own profit and sometimes on behalf of states.

This rapidly changing cyber landscape makes it difficult for governments, businesses, and other entities to adapt and defend themselves against the various aggressors in cyberspace. Despite numerous reports on the dangers of cyber attacks and a known history of computer-based espionage dating back to at least 1986, the Department of Defense still does not have a coordinated response to the problem.[7] It was not until 2009 that the Secretary of Defense directed the creation of US Cyber Command.[8] Yet despite its claim that it reached full operational capability in 2010, it is still trying to fill its six thousand positions.[9] This stands in stark contrast to the formation of the Computer Emergency Response Team in 1988 at Carnegie Mellon University's Software Engineering Institute after the discovery of the Morris worm.[10]

---

[6] Pascal-Emmanuel Gobry, "The Internet Is 20% Of Economic Growth," *Business Insider*, May 24, 2011, accessed October 2, 2014, http://www.businessinsider.com/mckinsey-report-internet-economy-2011-5?op=1.

[7] Clifford Stoll, "Stalking the Wily Hacker." *Communication of the ACM*, (May 1988): 490, accessed October 2, 2014, http://pdf.textfiles.com/academics/wilyhacker.pdf.

[8] "U.S. Cyber Command," US Cyber Command Public Affairs, August 2013, accessed October 2, 2014 http://www.stratcom.mil/factsheets/2/Cyber_Command/.

[9] Cheryl Pellerin, "Rogers: Cybercom Defending Networks," August 18, 2014, accessed October 2, 2014, http://www.defense.gov/news/newsarticle.aspx?id=122949.

[10] "CERT: About Us," Carnegie Mellon University, 2014, accessed October 2, 2014 http://www.cert.org/about/.

In 2007, Russian hackers attacked the Estonian government's computer networks in response to the announcement to move a monument dedicated to Soviet soldiers killed in World War II. The Russian government denied involvement and claimed it could not assist because of procedural issues with the Estonian government's requests.[11] In 2010, Stuxnet crippled the Iranian uranium enrichment program at Natanz by making the centrifuges operate so erratically that they destroyed themselves. Iran either could not identify or could not decisively respond to its attacker. The anonymity offered by cyberspace offers plausible deniability to attacking states or organizations. Both of these cases illustrate the difficulties with protecting critical cyber infrastructure and how to counter threats.

However, when attribution is possible, governments can respond appropriately for either defense or counter-attacking the cyber actors responsible. After a series of attacks on government and non-government computer systems, the US government took legal action against members of a group called LulzSec. Law enforcement agencies in the United States and Great Britain arrested the majority of this group, leading to its breakup. Despite off-shoots that attempt to appropriate its name for attention or tribute, LulzSec has not succeeded in mounting any significant attacks since the arrests. These legal actions have cooled the activity of groups like LulzSec because many of the members of these groups are not willing to risk time in prison to advance their political or personal agendas.

Research Question

What are the effects of delayed or denied attribution on deterring cyber attacks?

[11] Kertu Ruus. "Cyber War I: Estonia Attacked from Russia," The European Institute, December 02, 2007, accessed September 1, 2014, http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html.

Working Hypothesis

If a government is not possible to attribute a cyber network attack in a timely manner, then its response will be ineffective and will increase the probability of attacks in the future.

Significance of Research

The increasing use of information technology leads to dependence on this technology and thus vulnerability. Individuals, non-state actors, and states will increasingly use the cyber attacks to strike at the United States of America because of the ease of attack, low cost of entry, and perceived anonymity of cyberspace. Planners must understand the role and limits of deterrence to provide better options to national leadership when confronting threats in cyberspace. By examining state responses and their effects in previous cyber attacks, this paper seeks to identify the usefulness of deterrence at increasing the perceived cost and level of anonymity in cyber attacks.

Organization of Paper

The second section of this paper will examine the literature and theories that have already examined the nature of cyber attacks and the role of deterrence. The third section of this paper will discuss the research methods selected for this study. The fourth section reviews the three incidents (2007 Estonian cyber attacks, Stuxnet, and LulzSec) and their outcomes in relation to a defender's ability to attribute the attack, response, and its effectiveness for future deterrence. The fifth section presents analysis of the three case studies and their significance. The sixth section examines counterarguments and opportunities for further study. The final section presents conclusions drawn from the three case studies.

Literature Review

Cyber Theory

In 1989, William Lind and several co-authors wrote about the advent of Fourth Generation Warfare.[12] Although some authors have argued against this controversial concept as simply reinventing insurgency, it was one of the first academic articles to discuss the use of malicious software in conflict.[13] The ideas were still new at this point and the authors focused equally on the psychological component of disinformation as on the technical aspects of disrupting communications through malicious software.

Later, John Arquilla and David Ronfeldt further articulated the concept of cyber warfare in their 1993 article, “Cyberwar is Coming!” They discussed the implications of the proliferation of information technology and the critical role of information dominance in warfare. Writing after the decisive US-led coalition victory of Operation Desert Storm, the new concepts of cyber warfare and netwar were parts of the revolution in military affairs lauded for the one-sided defeat of the Iraqi Army.[14]

The United States was not the only country investigating the possible use of computers as weapons. In 1995, the Russian government declared that cyber war is a non-military phase of conflict and that it would respond overwhelmingly to the provocation, to include the potential

---

[12] William S. Lind, et al., "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette* 85, no. 11 (November, 2001): November 2001, accessed November 13, 2014, https://lumen.cgsccarl.com/login?url=http://search.proquest.com.lumen.cgsccarl.com/docview/221496693?accountid=28992.

[13] Antulio J. Echevarria II, "Fourth-Generation War and Other Myths," Strategic Studies Institute, November 2005, accessed November 13, 2014, http://www.strategicstudiesinstitute.army.mil/pdffiles/pub632.pdf.

[14] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" RAND, (November 1993): 23, 39, accessed December 7, 2014, http://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf.

first use of nuclear weapons.[15] In the early 1990's Russian theorists began discussing using malware as a force multiplier in future conflicts.[16]

No later than 1996, China began developing its cyber capabilities because it concluded cyber attacks are a legitimate part of asymmetrical warfare.[17] Two People's Liberation Army colonels, Qiao Liang and Wang Xiangsui, co-wrote *Unrestricted Warfare*, a guide to fighting a technologically and militarily more advanced enemy. In this text, they discussed the future of conflict involving all means available to their country to even the odds against the United States and how to turn some of its strengths into weaknesses. They included in their list of weapons "electromagnetic energy weapons for hard destruction or soft-strikes by computer logic bombs, network viruses, or media weapons." In addition to the use of computers, the authors blurred the lines between civilian and military by denying that there would be such a thing as "non-battlespace" once they included computer rooms and stock exchanges in their list of targets for opening attacks. Among the targets they recommend for early cyber attacks are the financial markets, civilian power grid, communications and mass media systems, and traffic control systems.[18]

Deterrence Theory

Although it pre-dated the Cold War, deterrence theory gained prominence then because of theorists like Bernard Brodie and Herman Kahn. The concept had existed since man began

---

[15] Steven A. Hildreth, "Cyberwarfare," in *Cyberwarfare: Terror at a Click*, ed. John V. Blane, (Huntington, NY: Novinka Books, 2001) 13-14.

[16] Timothy Thomas, "Russian Views on Information-based Warfare," Foreign Military Studies Office, July 1996, accessed December 2, 2014, http://fmso.leavenworth.army.mil/documents/rusvuiw.htm.

[17] Hildreth, "Cyberwarfare," 13-15.

[18] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Panama City, Panama: Pan American Publishing Company, 2002), 19-20, 31-32, 38-40, 123.

fighting, but it became far more important when dealing with the absolute nature of nuclear warfare.[19] Prior to the advent of nuclear weapons, the time required to raise an army of suitable size and transport it to an enemy nation varied from days to months.[20] These longer timelines gave ample response time once a defender detected the indicators of the attacker's strategic mobilization.

Additionally, the total destruction of cities was historically a byproduct of a siege or the conventional fighting in and around them, not the objective of the deliberate targeting population centers. Rulers and commanders did not want to destroy that which they wished to capture.[21] This changed with the advent of Total War and airpower, when civilians and industrial centers became targets to break the resistance of the opposing government.[22] After 1945, bomber and missile-delivered nuclear weapons could destroy entire cities in hours or even minutes after the decision to attack. These incredibly short timeframes during which a nuclear confrontation could escalate required a framework capable of defining the relationship between two nuclear-armed opponents and the terms of the relationship to prevent unintentional total annihilation.[23]

Likewise, cyber attacks have further decreased the reaction time, with attacks occurring at the speed of electrons or photons moving across the network.[24] This compression of timelines from decision to outcome makes some nuclear weapons policies and theories attractive to

---

[19] Lawrence Freedman, *Deterrence* (Malden, MA: Polity Press, 2004), 7, 10-11, 35.

[20] Michael Sheehan, "The Evolution of Modern Warfare," in *Strategy in the Contemporary World*, eds. John Baylis, James J. Wirtz, and Colin S. Gray, (Oxford: Oxford University Press, 2013), 41-42.

[21] Sheehan "The Evolution of Modern Warfare," 41.

[22] Azar Gat, *A History of Military Thought* (New York: Oxford University Press, 2001), 593; Sheehan "The Evolution of Modern Warfare," 50-52.

[23] Freedman, *Deterrence*, 16-17.

[24] John B. Sheldon, "The Rise of Cyberpower," in *Strategy in the Contemporary World*, eds. John Baylis, James J. Wirtz, and Colin S. Gray, (Oxford: Oxford University Press, 2013), 310.

planning for cyber operations. Some authors, like Richard Clarke, call for similar international agreements to establish either limits on attacks or communication procedures in cyber war similar to strategic arms treaties dealing with nuclear weapons.[25]

A final similarity between nuclear and cyber conflict is the inclusion of nearly everyone as a potential victim. Although it is possible for an attacker to discriminate between targeted computer systems, it is unlikely to exclude other systems entirely, especially of attackers are trying to disguise the attack's origin. Hackers may surreptitiously take over other users' computers to assist in the attack or deny attribution, regardless of whether the systems' owners are involved in the conflict. Malicious software can get out of control and spread, like the drift of fallout after a nuclear war, affecting belligerents as well as populations outside the target area. Similar to a generalized nuclear war, it will be nearly impossible for states and individuals to "opt out" and assume their refusal to participate prevents victimization.

There are, however, some major distinctions between cyber and nuclear war. The first is the far lower barrier to entry into cyber war. Whereas a nuclear weapons development program costs billions of dollars, developing a credible cyber capability is far less.[26] Secondly, it is easier to justify to the international community the development of a team of computer security experts than it is to justify building a nuclear bomb. A third distinction is the possibility of cyber conflict to occur without anyone knowing – hardly possible with nuclear warfare. Lastly, governments do not have a monopoly on cyber capabilities since a great deal of computer security and software development skills reside in the private sector.

To facilitate future discussion, it will be important to summarize quickly the basic principles of deterrence. The objective of deterrence is to prevent an opponent from pursuing a course of action that the defender does not want the opponent to. To make deterrence work, the

---

[25] Richard A. Clarke and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins Publishers, 2010), 268-271.

[26] Sheldon, "The Rise of Cyberpower," 309.

concept relies on the defender having the three “C’s” of capability, credibility, and communication. Capability means that the defender can carry out the action to deter the opponent. Credibility is the defender possessing sufficient will to execute the threat. Communication means that the defender must inform the opponent that it has the capability and the will to use it in response to the unwanted actions.[27]

Deterrence works through either denial or punishment. Denial tries to control the situation sufficiently to deprive the opponent of strategic choices. Punishment seeks to coerce the opponent not to choose the option that is still available.[28] The defending party seeks to increase the cost of the action to an unacceptably high level, lower the level of benefit, or lower the likelihood of success to change the cost-benefit analysis against the aggressor’s favor. Or as Gary Schaub wrote it in a formula: expected value = [benefits – costs] * probability.[29]

Cyberdeterrence

According to Amit Sharma, the deter phase of a conflict attempts to shape “the future conflict by gaining a credible and known deterrence.”[30] As other authors, such as Martin Libicki, have pointed out, the covert nature of cyber attacks frequently precludes the communication of

[27] T. V. Paul, "Complex Deterrence: An Introduction," in *Complex Deterrence: Strategy in the Global Age*, eds. T. V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago, IL: The University of Chicago Press, 2009), 2.

[28] Freedman, *Deterrence*, 37.

[29] Gary Schaub Jr., “When Is Deterrence Necessary? Gauging Adversary Intent," *Strategic Studies Quarterly*, Winter 2009, accessed December 7, 2014, http://search.proquest.com.lumen.cgsccarl.com/docview/1429444718?pq-origsite=summon.

[30] Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, eds. Christian Czosseck and Kenneth Geers (Washington, DC: lOS Press, 2009), 11.

deterrent threats.[31] This contradiction undermines the current state of cyber deterrence based on counterstrike within traditional deterrence models. The defender needs his opponent to understand he has a capability and the willingness to use it without openly communicating it.

An author's view of the threat informs his decision about the appropriate deterrent counter-threats. There tend to be three camps in general: Minimalists, Moderates, and Alarmists. Minimalists do not require much explanation because they are the authors who believe that cyber does not pose any significant threat. Moderates explain that cyber provides new capabilities but these will not win any wars by themselves. Lastly, the alarmists are the authors who write about hacked computer systems killing thousands and warn of an impending "cyber-attack that could be the equivalent of Pearl Harbor" or a "Cyber Armageddon."[32]

Amongst the minimalists are Lawrence Freedman and Thomas Rid. Freedman grants discussion of cyber attacks a scant two pages in his seven hundred fifty-one page compendium of strategic theory and lumps most cyber attacks together with information warfare or criminal activity. Thomas Rid dismisses cyber warfare as "more hype than reality" since no one has died from a cyber attack yet.[33] He argues it is a "wasted metaphor" since most events are non-violent and are just updated versions of sabotage, espionage, or subversion.[34] As a result, law enforcement authorities should prosecute individuals committing computer crimes and

---

[31] Martin C. Libicki, "Sub Rosa Cyber War," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, eds. Christian Czosseck and Kenneth Geers (Washington, DC: lOS Press, 2009), 58.

[32] Leon E. Panetta, "Remarks by Secretary Panetta to Service Members at US Strategic Command," US Department of Defense, August 5, 2011, accessed November 13, 2014, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4861; Daniel Goure. "Prepare for Cyber Armageddon," *The Lexington Institute*, December 9, 2014, accessed December 15, 2014, http://www.lexingtoninstitute.org/prepare-for-cyber-armageddon/.

[33] Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, February 27, 2012, accessed November 13, 2014, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar.

[34] Lawrence Freedman, *Strategy: A History* (New York: Oxford University Press, 2013), 229-230.

government authorities should be able to continue operations, albeit at a degraded level of efficiency. Former Obama administration Cybersecurity Coordinator, Howard Schmidt, also stated in interviews that the threat seemed exaggerated and he likened most of the online attacks to street protests that may temporarily impede traffic in a city.[35] These authors have typically not addressed the proven destructive capabilities of some cyber attacks.

On the other side of the spectrum are the alarmists, who describe catastrophic attacks akin to nuclear attacks in their speed and disruption. Richard Clarke and Robert Knake describe a scenario in which cyber attackers shut down the entire continental United States with a nationwide blackout, derailed trains, exploding gas pipelines, out of control fires, and even the president stuck in a chaotic downtown Washington, DC paralyzed by gridlocked traffic. Despite this destructive capability, however, they flatly deny the capability of the United States to deter a cyber attack, citing on-going attacks.[36] Unfortunately, they appear to either conflate cyber attacks with cyber espionage or do not acknowledge there may be response criteria that have not been met. Daniel Goure also argues the dire consequences for unprepared US infrastructure and calls for doctrine and capabilities to deter attack or defend the country.[37] Timothy Thomas, similarly, sees value in a declared US offensive capability to deter foreign threats including persistent Chinese cyber espionage against the US government and private sector. He dismisses Rid's "no deaths means no cyber war" argument by comparing the harm of ongoing cyber attacks to the harm committed by the non-lethal attacks such taking hostages or emptying someone's bank

[35] Josephine Wolff, "Howard Schmidt: Hackers and spies have launched attacks on vital computer systems in recent months. White House cyber-security coordinator Howard Schmidt on what it all means," *Newsweek*, January 3, 2011, accessed December 7, 2014 http://search.proquest.com.lumen.cgsccarl.com/docview/822401947?pq-origsite=summon.

[36] Clarke and Knake, *Cyber War*, 64-68, 194-195.

[37] Goure, "Prepare for Cyber Armageddon."

account.[38] During a speech at US Strategic Command, former Secretary of Defense Leon Panetta said cyber attacks had the capability to take down the US power grid, financial systems, government systems, and banking systems to paralyze the country.[39]

As a result of these potential calamities, alarmist authors recommend far more comprehensive preventative measures than modest upgrades to network security. Clarke and Knake recommend establishing an “Obama Doctrine” that judges attacks based on their outcomes, not the means used to achieve them. This means the US government would treat a cyber attack causing an explosion on par with a terrorist attack or a warplane dropping a bomb. This prevents the attacker from denying malicious intent by claiming a non-violent computer intrusion was the cause. The US government would also hold other governments responsible for the actions of people or equipment operating within their territory.[40] This recommendation is similar to the authors of *The Sovereignty Solution*, whose parsimonious approach to foreign policy holds foreign governments accountable for activities, such as terrorism or cyber attacks, originating in their state. Failure to control these activities implies either an inability to handle the situation or support from that government. The US government would offer support to a government that lacked the capacity, but coercive actions would follow an unwillingness to stop the attacks.[41]

---

[38] David Feith, "Timothy Thomas: Why China Is Reading Your Email; Beijing's cyber attacks are rooted in military strategy, says one of America's foremost experts. The best way to combat them is for the U.S. to go on the cyber offensive too," ProQuest, March 29, 2013, accessed December 2, 2014, http://search.proquest.com.lumen.cgsccarl.com/docview/1321561425?pq-origsite=summon.

[39] Panetta, "Remarks by Secretary Panetta to Service Members at US Strategic Command."

[40] Clarke and Knake, *Cyber War*, 178.

[41] Anna Simons, Joe McGraw, and Duane Lauchengco, *The Sovereignty Solution: A Commonsense Approach to Global Security* (Annapolis, MD: Naval Institute Press, 2011), 50.

Between these two groups are the moderates, including writers like John Sheldon, Colin Gray, and Daniel Moran. These authors recommend that governments take prudent measures to protect their networks and even critical infrastructure. Gray acknowledges the expense of redundancies and backups but explains them as necessary security investments. He also acknowledges the impossibility of securing everything, but denies the fatalism some alarmists imply by hedging with measures to prioritize some systems over others and promote resiliency after an attack. "Good practice in cyber security includes preparation to suffer some disruption, but then to recover rapidly. Not seriously impaired."[42] Ultimately, states will continue to use cyber capabilities in coordination with other forms of national power.[43] Playing on the name of a recent James Bond movie *Skyfall*, in which a hacker conducts catastrophic cyber attacks leading to explosions in downtown London, Colin Gray concludes "…the sky will not fall because of hostile action against us in cyberspace unless we are improbably careless and foolish."[44]

While not delving into the immediacy of how to defend against attacks, some authors have instead examined the legality of actions defenders can take during or after an attack. Jay Kesan and Carol Hayes's thorough review of the legal framework for responding to a cyber attack recommends the use of defensive means and criminal liabilities rather than the victim counterattacking. If a victim chose to counterattack, as a last resort, it must meet very high standards for attribution and discrimination to prevent damage to third party computer systems.[45] Hannah Lobel likewise identifies the law of war issues of proportionality, distinction, and the use

---

[42] Colin Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle, PA: U.S. Army War College Press, 2013), 43; *Skyfall*, directed by Sam Mendes (Twentieth Century Fox, 2012), DVD (Twentieth Century Fox, 2013).

[43] Daniel Moran, "Geography and Strategy," in *Strategy in the Contemporary World*, eds. John Baylis, James J. Wirtz, and Colin S. Gray (Oxford: Oxford Univesity Press, 2013), 129.

[44] Gray, *Making Strategic Sense of Cyber Power*, 52.

[45] Jay A. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," Social Science Research Network, April 7, 2011, accessed November 15, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1805163, 486-487.

of force in the context of cyber attacks. She uses Stuxnet as an example of how malicious code can spread far beyond its intended target, but asserts well-designed code will only execute on the targeted system.[46]

Both sets of authors have raised the question of what options non-governmental entities have to respond to attacks. Many private sector computer security professionals are simply concerned with returning their network to normal functionality.[47] However, Lobel, Kesan, and Hayes address the issue of private sector companies counterattacking instead of simply taking defensive actions on their own networks. With increasingly effective methods of attack available to hackers and increasing costs to the defenders through infrastructure, theft, fraud, and extortion, it is within the realm of possibility that a victim could choose to fight back. Kesan and Hayes state that a "mitigative counter-strike" could be legal as long as it affected only the attacker's system and was limited to disrupting the attack. Raising the attribution standard for response, they assert that attribution technology does not currently provide this level of accuracy.[48]

While these methods may be appropriate for controlling rogue elements in the private sector, they may not be for all incidents. When critical infrastructure or high priority government systems are the victims since the effects could include loss of life or massive economic disruption so the demands for response are greater. As with most military operations, the defenders will only have partial information but will still have to decide, possibly with just enough information to satisfice. If government officials make this "good enough" decision, instead of private sector business executives, it could also include input from information Kesan and Hayes did not consider. Multi-disciplinary intelligence not available outside the government can corroborate

---

[46] Hannah Lobel, "Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict," *Texas International Law Journal*, Volume 47, Issue 2-3 (Summer 2012), accessed December 7, 2014, http://search.proquest.com.lumen.cgsccarl.com/docview/1018566780?pq-origsite=summon.

[47] Clarke and Knake, *Cyber War*, 213.

[48] Kesan and Hayes, "Mitigative Counterstriking," 485.

incomplete technical data from network administrators to aid attribution. Furthermore, since these authors only endorse “mitigative counter-striking” to stop the attacking system or systems, they overlook the possibility of using a counterattack to punish the attacking party by responding in a proportional manner to increase the cost of attacking. This would offset the low cost of entry and perceived anonymity that cyber attacks offer but may still be within the realm of government authority, similar to the use of military force.

Martin Libicki argues that traditional deterrence and deterrence in cyberspace are different because of the differences between nuclear deterrence and cyberdeterrence. Among some of his concerns are private sector accountability, the difficulty of attribution, and the dangers of escalation. He asserts that placing businesses and critical infrastructure under the deterrent umbrella of government counterattack could lower overall security because private sector entities will not invest in securing their systems if they perceive the government will defend them. [49] Although his concerns about the difficulties of attribution are fair, his analogy that escalation does not exist for the use of nuclear weapons is ambiguous. Although it is not possible to escalate above nuclear war, he seems to imply that any use of a nuclear weapon leads to immediate commitment of a state’s entire nuclear arsenal. Nuclear options are not as black and white and permit for posturing, controlled escalations, and limited exchanges. Cyber gives the ability to migrate from its domain to physical attacks, but it also allows for limited or widespread attacks resulting in real-world damage.

For a state with many conventional military advantages, such as the United States, escalation outside of the cyber domain could prove to be a very useful part of its deterrent policy in cyber warfare. To prevent the use of an unknown cyber attack technique and hence render it less useful in the future, the United States could choose to use non-cyber means to respond to a

[49] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: Rand Project Air Force, 2009) 41, 64-69, accessed December 7, 2014, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

cyber attack. Any of the usual instruments of national power could be used to deter an attacker, including presenting a case to the World Trade Organization to counter industrial espionage, arresting the hackers, instituting economic trade sanctions, seeking international censure, or military attacks. The key to these responses, however, is being able to attribute in public the actions of the attack to a political actor.

Nonetheless, Martin Libicki developed a very useful decision loop for responding to cyber attacks.[50] (See Figure 1) This chart illustrates very well the choices available to the United States government when responding to alleged cyber incidents. As the examples in the case studies will show, each government responding to a cyber attack evaluates its situation and response in a similar manner.

Unfortunately, there have been very few case studies that examine the practical effect of these various abstract theories. While many authors have discussed the possibilities of cyber attacks and many have lamented the vulnerabilities, there have not been any comprehensive studies of how defenders can use policy to prevent cyber attacks. This paper will examine three different cases to determine the effectiveness of cyber defense, the effect of attribution on deterrence, and the policy implications of the conclusions drawn.

[50] Libicki, *Cyberdeterrence and Cyberwar*, 99.

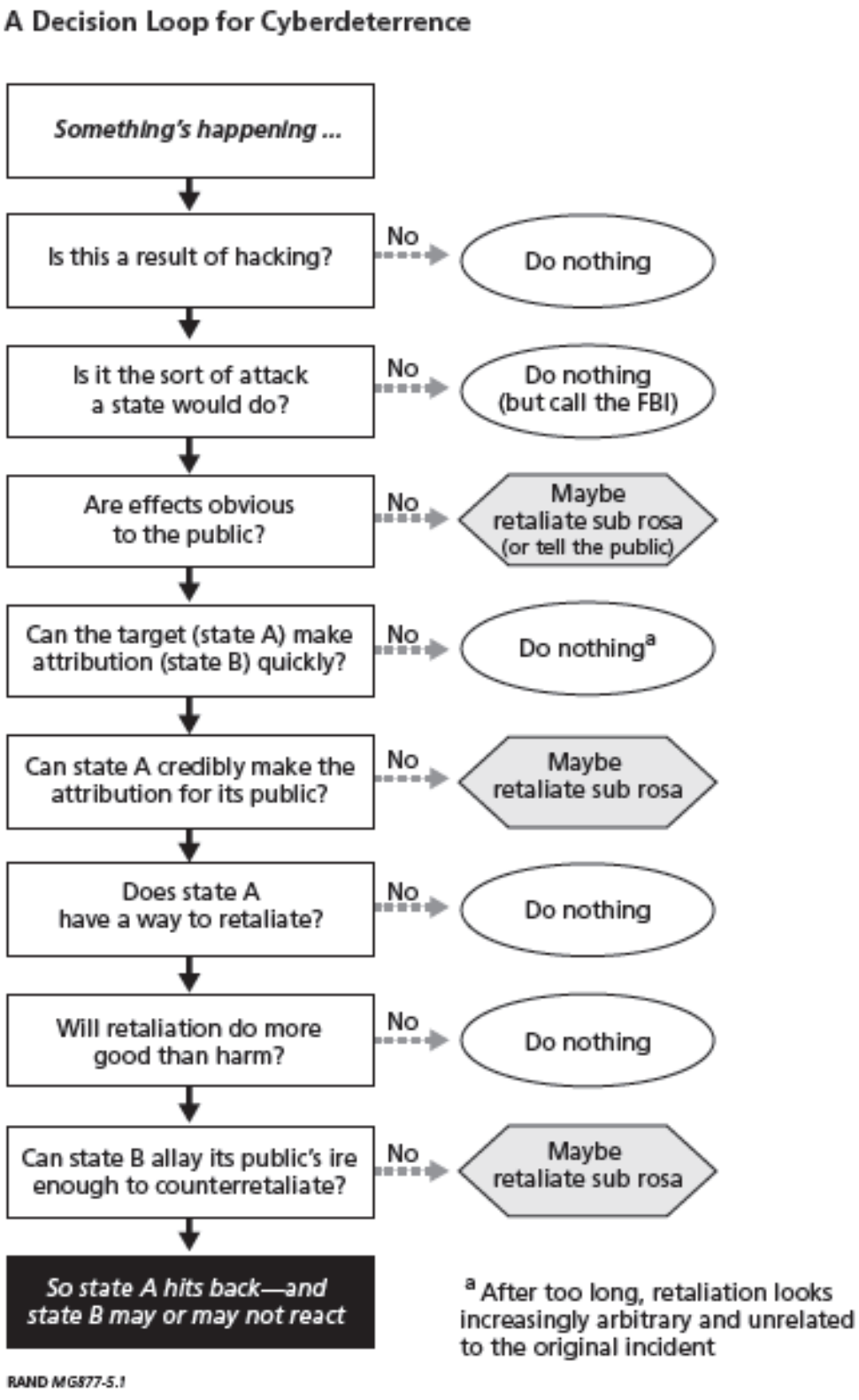

Figure 1: Martin Libicki's Decision Loop for Cyberdeterrence

Source: Libicki, *Cyberdeterrence and Cyberwar*, 99.

Methods

Case studies provide the opportunity to observe real world events and apply existing theories to them.[51] They can test theories, create theories, identify antecedent conditions, test the importance of these antecedent conditions, and explain cases of intrinsic importance. Case studies use three different formats: the controlled comparison, congruence procedure, and process tracing.[52]

Since cyber attacks are a relatively new phenomenon, there is not a well-developed history of the attacks or analysis thereof. The lack of transparency of cyber attacks further complicates analysis. Many organizations, if they are even aware they are the victim of an attack, do not release the information to the public out of fear of additional attacks, loss of stakeholder confidence, or embarrassment.

This paper utilizes controlled comparison to review three separate case studies of cyber attacks from the last ten years and analyze the actions of the attacker, the defender, the outcome, and implications from each attack. The qualitative review of these three events will examine the circumstances of the event, the ability for the defender to attribute the attacks in a timely manner and to offer a credible response to the attack, and the effects on future attacks. Since the three cases are all different, it may not be possible to identify trends from them. However, it may be possible to possible to identify different types of reactions and implications in different kinds of cyber attacks.

From the last fifteen years, there have been multiple cases of coordinated cyber attacks that are available for public review. This paper will not examine routine malware, used for criminal financial gain or mischief, since there is no ascertainable political objective. Instead, it will examine three coordinated events that had stated political objectives. The differences

---

[51] Stephen Van Evra, *Guide to Methods for Students of Political Science* (Ithaca, NY: Cornell University Press, 1997) 50.

[52] Van Evra, *Guide to Methods for Students of Political Science*, 55-56.

between the events, however, will provide for the examination of the variables of attribution, state sponsorship, and policy options available.

Although there are many cyber attacks to study, many are inappropriate for this monograph. The 2008 attacks on Georgia had a conventional military component, making them dissimilar to the three events examined. The 2014 attack on Sony is too recent and significant amounts of information are not available or conflict. The Advanced Persistent Threat 1 reported by Mandiant and the Iranian penetrations reported by Cylance both appear to be cases of espionage, not offensive cyber attacks.

Case Studies

This section reviews the three aforementioned case studies. The examples of the 2007 attack on Estonia and Stuxnet both demonstrate the abilities of cyber attacks against nation states, whereas LulzSec shows how the actions of non-state actors can frustrate the actions of both private and public sector organizations. All three cases show how governments have responded to cyber attacks, despite varying degrees of attribution, capabilities, and political will.

Estonia

In 2007, the Estonian government announced plans to move a monument commemorating the Soviet Union's war dead. In decades past, veterans of the Soviet armed forces used the memorial as a meeting place on civic holidays. More recently, hooligans used it to meet prior to engaging in "unruly, violent anti-Estonian protests" when Russia voiced opposition to the European Union. To prevent further disturbances, the Estonian government decided to relocate it from downtown Tallinn to the military cemetery at dawn on April 27, 2007. As uncontroversial as this may seem, the Russian government and the 400,000 strong Russian minority in Estonia voiced strong opposition to this. Some of these protests degenerated into anti-

Estonian riots. Rioters threw Molotov cocktails, looted, burned cars, and stabbed one person to death.[53]

On the night before the statue's move, a sustained attack on numerous government information systems began shortly before midnight on April 26, 2007. These attacks, known as a Distributed Denial of Service (DDoS), flooded the computer systems with more connections than they could handle and eventually made the systems unresponsive to normal users. A DDoS is uncomplicated and easy to execute, but usually requires a large number of coordinated computers to overwhelm the targeted systems. These attacks require either a massive number of individuals attacking simultaneously or a network of computers, known as a botnet, covertly controlled through a backdoor to execute commands unknown to their owners.[54]

Either way, the attack requires some form of command and control. In Estonia's case, websites hosted on servers located within Russian posted instructions on how and what to attack. Attackers, or their sympathizers, created Paypal accounts to collect donations to hire botnets to conduct the attack.[55] These attacks coincided with actual street riots involving thousands of ethnic Russians living in Estonia and calls by the Russian government for the Estonian government to resign for what it called "blasphemy."[56]

Security experts have divided the attack into two phases. During the first phase, amateurish attacks defaced websites or posted fake letters of apology from Estonian officials online. The second phase, however, included a more sophisticated DDoS attack assessed as the

---

[53] Ruus, "Cyber War I: Estonia Attacked from Russia."

[54] Felix Leder, Tillmann Werner, and Peter Martini, "Proactive Botnet Countermeasures: An Offensive Approach," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, eds. Christian Czosseck, Kenneth Geers (Washington, DC: IOS Press, 2009), 211.

[55] Ruus, "Cyber War I: Estonia Attacked from Russia."

[56] "A Cyber-Riot," The Economist, May 27, 2007, accessed September 1, 2014, http://www.economist.com/node/9163598.

work of expert hackers.[57] This phase required the deployment of a botnet of over a million computers to flood the country with more than one thousand times its normal internet traffic. [58]

Members of the Kremlin's official youth movement, Nashi, claimed credit for the attacks.[59] Despite Moscow's heated rhetoric, a State Duma member's claim of responsibility, Nashi's involvement, and a failure to prosecute anyone who has claimed credit for the attack, the Russian government has denied responsibility.[60] To dismiss the forensic evidence, Russian security officials speculated that attackers could have falsified Russian Internet Protocol addresses for the attack.[61] When Estonia requested assistance in stopping the three-week long attack, Russia refused and cited procedural issues with the requests.[62] The Estonian government, fearful of escalating the matter, never directly attributed the attack to the Russian government.[63] Additionally, if the Estonians had considered counterattacking in cyberspace, it is likely they quickly discarded the idea either because of the Russia government's highly proficient cyber capabilities or conventional military overmatch. [64]

---

[57] Chloe Arnold, "Russian Group's Claims Reopen Debate On Estonian Cyberattacks," *Radio Free Europe / Radio Liberty*, March 30, 2009, accessed September 30, 2014, http://www.rferl.org/content/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html.

[58] Ruus, "Cyber War I: Estonia Attacked from Russia."

[59] Noah Shachtman., "Kremlin Kids: We Launched the Estonian Cyber War," *Wired*, March 11, 2011, accessed September 30, 2014 http://www.wired.com/2009/03/pro-kremlin-gro/.

[60] Arnold, "Russian Group's Claims Reopen Debate On Estonian Cyberattacks."

[61] Binoy Kampmark, "Cyber Warfare Between Estonia and Russia," *Contemporary Review* (Autumn 2007) 291, accessed December 7, 2014, http://search.proquest.com.lumen.cgsccarl.com/docview/204958799/fulltextPDF?accountid=28992.

[62] Ruus, "Cyber War I: Estonia Attacked from Russia."

[63] Kampmark, "Cyber Warfare Between Estonia and Russia," 291.

[64] Clarke and Knake, *Cyber War*, 21.

The effect on this country of 1.3 million was disruptive, but not destructive. Estonia has one of the most electronically advanced populations on the planet. The Estonian government issues electronic identity cards that enable their citizens to vote, pay taxes, pay parking meters or bus fare, and view their children's grades on-line.[65] Estonian computer programmers invented both the Skype video-teleconferencing software and Kazaa peer-to-peer file sharing software. In 2007, Estonians began voting in national elections online, as well as conducting eighty-five per cent of banking online.[66] With this level of information technology integration, the attack disrupted some services and surely annoyed many Estonians, but did not prove to be a major national security threat.

Eventually, the Estonian CERT developed a three-pronged approach to fixing the problems. The first step was to increase the server capacity for their systems to handle more traffic. The second step was to develop a filtering system to separate good message traffic from bogus message traffic associated with the attack. The third and final step was to work with authorities responsible for the root Domain Name System servers to take the identified botnet computers offline.[67] Unfortunately, Estonia had to close its computer systems off from access outside of the country. This effectively sacrificed the country's connectivity to the rest of the world, so Estonian citizens inside its borders could still access these essential modern services.[68] If the intent was to disrupt the Estonian government's ability to communicate, then the attackers achieved their goals when the government removed these systems from international connectivity.

---

[65] Kertu Ruus, "E-Stonia: Pioneer of Internet Innovation and e-Goverment." The European Institute. March 2, 2007, accessed September 1, 2014, http://www.europeaninstitute.org/20070302100/Spring-2007/estonia-pioneer-of-internet-innovation-and-e-goverment.html.

[66] Ruus, "E-Stonia: Pioneer of Internet Innovation and e-Government."

[67] Ruus, "Cyber War I: Estonia Attacked from Russia."

[68] Libicki, *Cyberdeterrence and Cyberwar*, 1.

While this seems relatively harmless, it can be very dangerous when coupled with other actions. The conflict in between Russia and Georgia in 2008 illustrates how a DDoS attack can support conventional military operations by disrupting communications on the eve of war. For three weeks prior to Russia's invasion, hackers attacked many of the Georgian government's computer systems.[69] It does not require much to imagine the disorder this caused as war loomed.

The inability of Estonia to attribute the attacks directly to the Russian government and its inability or unwillingness to escalate the situation means the attackers got away with it. With only one Estonian charged in connection with the attacks, the perpetrators received no punishment. From a cost-benefit analysis, the attackers had little to no cost but a great deal of benefits. If the objective was to show countries that share a border with Russia that they have to continue to respect the wishes of their former Soviet-era occupier, the coordinators of the attack very clearly demonstrated it. If the attack was a probe of security of western countries and their resolve, then the attackers were able to observe the response to their attacks. And if the attack was a rehearsal for a larger attack, coordinated with a physical invasion, then the technique was well proven and expanded for the attacks on Georgia.

Stuxnet

In 2010, a new malware program named Stuxnet made its way through the internet looking for a very specific set of computers to attack.[70] It took a team from anti-virus maker Symantec over seven months to determine that this program was searching for computers that

[69] Noah Shachtman, "Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It," *Wired*, March 11, 2009, accessed October 5, 2014, http://www.wired.com/2009/03/georgia-blames/.

[70] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, accessed October 8, 2014, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

controlled uranium enrichment equipment in Iran based on the information from the sample of the program they had.[71] Their sleuthing needed help from partners in multiple countries and across the information technology industry. Rand Beers, the Under Secretary for the National Protection and Programs Directorate at the Department of Homeland Security, called Stuxnet a "first of its kind" weapon.[72] It used four different unknown software vulnerabilities, including the first programmable logic controller rootkit, and specifically targeted one country's nuclear technology sector for destruction.[73] This was the dawning of a new era – the era of the precision guided e-bomb.

Stuxnet attacked supervisory control and data acquisition (SCADA) systems controlling Iranian uranium centrifuges. After someone introduces it into the computer system by using a memory stick to cross the air gap to computers not connected to the internet, it identifies that it is on the proper system and spreads to other computers through shared printers.[74] During the next phase, it determines what normal operations are and records the data. While this information could be interesting for espionage purposes, the real reason Stuxnet records this information is for deception.[75]

Once Stuxnet goes from passive to active, it plays this pre-recorded information to the personnel monitoring the uranium enrichment process so they will think that operations are

---

[71] "Duqu: The Precursor to the Next Stuxnet," Symantec, accessed November 30, 2014, http://www.symantec.com/outbreak/?id=stuxnet.

[72] Irving Lachow, "The Stuxnet Enigma: Implications for the Future of Cybersecurity," *Georgetown Journal of International Affairs*, (Fall 2011), 120.

[73] Liam O Murchu, "A Malware Anniversary to Remember," *Symantec: Security Response*, July 11, 2011, accessed November 30, 2014, http://www.symantec.com/connect/blogs/malware-anniversary-remember.

[74] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, accessed October 8, 2014 http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/.

[75] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."

continuing like normal. While the centrifuges are spinning erratically and tearing themselves apart, the monitoring personnel are unaware of the problem because the pre-recorded data displayed on their computers. As a finishing touch, Stuxnet deletes itself from the system to cover its tracks.[76]

Given the assumptions that Iran is refining uranium to develop a nuclear weapon, it is unlikely the Iranians would truthfully report the nature of the attack or how they responded. Iranian officials have issued mixed messages, calling the attack not serious while claiming to have arrested nuclear spies.[77] Some reporters have speculated that the Iranian scientists did not even know a hostile computer program was destroying their equipment. Instead, they tried to discover a technical glitch, as if their centrifuge failures were a normal part of the refining process.[78] Incredibly, one version or another of Stuxnet had been operating on Iranian computers as far back as 2008 without detection.[79] It was not until an international team of malware investigators published their findings on Stuxnet that the Iranians clearly understood a hostile cyber force had attacked their facility.[80] Some analysts have estimated the attack cost Iran between eighteen months and three years in its nuclear weapon development timeline.[81]

One of the biggest problems with Stuxnet, as with other malware, is that it did not stay on

---

[76] Lobel, "Cyber War Inc.," 632.

[77] Michael J. Gross, "A Declaration of Cyber-War," *Vanity Fair*, April 2013, accessed December 4, 2014, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

[78] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."

[79] Rupert Goodwins, "Stuxnet has put us all on the front line of warfare 2.0," *ZDNet*, June 1, 2012, accessed October 8, 2014, http://www.zdnet.com/stuxnet-has-put-us-all-on-the-front-line-of-warfare-2-0-3040155333/.

[80] Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History."

[81] Kim Zetter, "Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force,'" *Wired*, March 25, 2013, accessed November 30, 2014, http://www.wired.com/2013/03/stuxnet-act-of-force/; Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."

the target system. Despite the best efforts of the code writers, it appears a mistake in a programming update caused the program to replicate itself on computers outside of Natanz.[82] The Symantec team that unraveled the mystery received a copy because other people found the program on their computer systems.[83] This also exemplifies one of the biggest concerns for offensive cyber operations planners – if a country decides to commit a cyber attack with a newly developed weapon, it cannot prevent this weapon from getting out and re-used.

Unlike traditional weapons that get used up over time, a cyber weapon can be copied an infinite number of times. Instead of consumption, obsolescence is its greatest enemy because users can fix the fault in the system or discontinue using the faulty system. A cyber attacker must carefully weigh the costs and benefits of exploiting a vulnerability in a computer system because doing so may call attention to the flaw, resulting in its correction. Similarly, once an attacker deploys a new malicious program, another hacker can reverse engineer the program, edit it to perform a new task, and use it against another target.

There are many other difficult issues when dealing with Stuxnet. Attackers needed to identify the location of the facility, determine the equipment inside, write the highly sophisticated malware program to exploit vulnerabilities in that equipment, test it, and then develop a way to introduce Stuxnet into the air-gapped system. This would require well-integrated intelligence and clandestine operations as elements of the overall project, leading many to believe that Stuxnet was a state-sponsored attack. Eugene Kaspersky, founder of the world's fourth largest computer security company, speculates the US government received assistance from Microsoft to write the program.[84] *The New York Times* claims Israel and the United States are responsible, under a

---

[82] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."

[83] Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History"; Gross, "A Declaration of Cyber-War."

[84] Gross, "A Declaration of Cyber-War."

program called “Olympic Games.”[85]

Israel and the United States certainly have an interest in preventing Iran from successfully producing highly enriched uranium. Although some legal experts specializing in cybersecurity consider Stuxnet an illegal “act of force” because it destroyed government equipment, it is nothing worse than what these three countries have done to each other over the past few decades.[86] Iran has sponsored terrorist and insurgents responsible for the deaths of hundreds of Israelis and Americans over the last thirty years and Israel is purported to have killed several high-ranking Iranian scientists involved in their nuclear weapons program.[87]

Stuxnet destroyed a great deal of equipment in the Iranian nuclear program, but it did so without death or injury of personnel. This is far different from the more lethal military operations that the US and Israel must have considered to prevent Iran from producing a nuclear weapon. Israel’s air strikes to destroy both the Iraqi nuclear program at Osirak in 1981 and the Syrian program at Al-Kibar in 2007 are examples of how far Israel will go to enforce the Begin Doctrine of preventing its enemies from obtaining nuclear weapons.[88]

Despite the Stuxnet attack beginning in 2008, it is not clear when the Iranians became aware of it.[89] Some reports indicate that Iranian scientists did not know what was wrong when their centrifuges began failing at higher than expected rates. Iran’s official reaction did not become public until 2010 and it was not until 2011 when Iran publically announced the creation of its own cyber unit capable of offensive operations. Brigadier General Gholamreza Jalali, chief

---

[85] Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran.”

[86] Zetter, “Legal Experts: Stuxnet Attack on Iran Was Illegal ‘Act of Force.’”

[87] Zetter, “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History.”

[88] “Isarael | Country Profile | Nuclear,” The Nuclear Threat Initiative, last updated May 2014, accessed October 25, 2014, http://www.nti.org/country-profiles/israel/nuclear/.

[89] Goodwins, "Stuxnet has put us all on the front line of warfare 2.0."

of Iran's Passive Defense Organization at the time, declared that Iran had the capability to fight its enemies in cyberspace.[90]

By making this announcement, Iran clearly indicated its intent to strike back at anyone who attacks it. This covers the communication component of a deterrent threat. Iran's cyber capability is most likely its greatest weakness in its deterrent threat. It is hard to doubt its willingness to follow through on threats since it has sponsored terrorist attacks throughout the world and appears to be responsible for multiple increasingly sophisticated cyber attacks since the discovery of Stuxnet.[91]

In August 2012, hackers inside Iran attacked the oil company, Saudi Aramco, and the Qatari natural gas company, RasGas. The "Shamoon" virus deleted important data on 30,000 Saudi Aramco computers. At the time, the US Secretary of Defense announced that the United States had improved its ability to trace digital attacks to their source. It also maintained the right to use a digital pre-emptive strike to protect vital cyber assets, underscoring its deterrent threat.[92] However, despite the attribution to actors within Iran, the United States never publically held Iran directly accountable for the attack.

A cyber security expert familiar with the incident explained that Shamoon appeared to be a reverse-engineered version of malware used against an Iranian energy company. An inside agent with privileged access installed the program, which led to millions of dollars in lost

---

[90] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."

[91] Greg Bruno, "State Sponsors: Iran," The Council on Foreign Relations, October 13, 2011, accessed November 20, 201,4 http://www.cfr.org/iran/state-sponsors-iran/p9362; Julian E. Barnes, and Siobhan Gorman, "U.S. Says Iran Hacked Navy Computers," *The Wall Street Journal*, September 27, 2013, accessed October 26, 2014, http://online.wsj.com/articles/SB10001424052702304526204579101602356751772.

[92] Agence France-Presse, "U.S. says Iran behind cyber attack in Saudi Arabia," *Al Arabiya News*, October 13, 2012, accessed October 26, 2014, http://english.alarabiya.net/articles/2012/10/13/243475.html.

productivity

and unforeseen expenses. Fortunately for the Saudi company, the attempted data theft failed and Shamoon simply deleted the data on the hard drives in an attempt to cover its tracks.[93]

The Shamoon incident displays two problems with offensive cyber operations and deterrence. The first problem is selecting the right response to the work of "amateurs." The Iranian government borrowed a page from the Russian playbook by sponsoring a third party to keep the incident at arms-length to deny attribution. The second problem is that defenders can reverse engineer and use the cyber weapons in the future, as shown by Shamoon's lineage from a program originally used against Iran.

After the Saudi Aramco and RasGas attacks, multiple businesses in the USA reported they were victims of sustained DDoS attacks. These attacks targeted businesses in the financial sector, such as JPMorgan, Bank of America, and Chase. Since Iran did not claim responsibility, analysts must infer the reason for the attacks from recent events that may have triggered the attacks. Some US government officials have speculated that the attacks were retaliation for western sanctions on Iran because of its nuclear program.[94] Since the attacks occurred just months after *The New York Times* article claiming confidential government confirmation of the US government's role in creating Stuxnet, it may be that these DDoS attacks were Iran's response to the attribution of the attack. Although the attacks were simply DDoS attacks against commercial websites, they may have been Iran's best effort at demonstrating its new capability and attacking what it sees as the US's center of gravity – its economy.

---

[93] Michael Lipin, "Saudi Cyber Attack Seen as Work of Amateur Hackers Backed by Iran," *Voice of America*, October 25, 2012, accessed October 26, 2014, http://www.voanews.com/content/saudi-arabia-iran-cyber-attack/1533694.html.

[94] Ellen Nakashima, "Iran Blamed for Cyber Attacks on U.S. Banks and Companies," *The Washington Post*, September 21, 2012, accessed September 7, 2014, http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html.

In 2012, Iran's capabilities were still low according to some US government officials.[95] This is plausible if the Iranian announcement of the creation of their cyber unit is taken at face value. If Iran did not create this unit until 2011, their capabilities would have been nascent and a DDoS may have been the best they could accomplish after one year. Since then, however, they appear to have significantly improved their capabilities. A year after the attacks on US financial companies, the US Navy reported that Iran had hacked into its email network and intranet.[96] It took the Navy four months to clear out the Iranian hackers from their systems completely.[97] This network penetration shows a higher level of skill and sophistication than previously seen from Iran and means that their capabilities have increased since the Stuxnet attacks. Most recently, a cybersecurity firm published a report claiming Iranian hackers has penetrated at least fifty different organizations in sixteen countries since 2012.[98] Many of those, including oil companies and airlines, have denied any compromise of their security.[99]

Perhaps, in the future, governments seeking to use offensive cyber operations to destroy Iranian equipment will have to think twice since Iran has developed more effective second-strike capabilities. At the time of Stuxnet, however, these capabilities did not yet exist so Iran could not

---

[95] Nakashima, "Iran Blamed for Cyber Attacks on U.S. Banks and Companies."

[96] Julian E. Barnes, and Siobhan Gorman, "U.S. Says Iran Hacked Navy Computers," *The Wall Street Journal*, September 27, 2013, accessed October 26, 2014, http://online.wsj.com/articles/SB10001424052702304526204579101602356751772.

[97] Mark Clayton, "Cyber-war: In Deed and Desire, Iran Emerging as a Major Power," *The Christian Science Monitor*, March 16, 2014, accessed October 26, 2014, http://www.csmonitor.com/World/Security-Watch/Cyber-Conflict-Monitor/2014/0316/Cyber-war-In-deed-and-desire-Iran-emerging-as-a-major-power.

[98] *Operation Cleaver*, Cylance, December 1, 2014, 5, accessed December 4, 2014, http://www0.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf.

[99] Michael Riley and Jordan Robertson, "Iran-Backed Hackers Target Airports, Carriers: Report," *Bloomberg*, December 2, 2014, accessed December 4, 2014, http://www.bloomberg.com/news/2014-12-02/iran-backed-hackers-target-airports-carriers-report.html.

make a credible deterrent threat even if it had already communicated its willingness to respond. The way the attackers deployed Stuxnet by memory stick also likely put attribution beyond Iran's attribution capabilities, delaying attribution until *The New York Times* article. The cost-benefit analysis clearly favored using Stuxnet against Iran, given the trade-off of some minor disruption of trade over the possibility of a nuclear-armed Iran.

LulzSec

New technologies introduce new capabilities that can empower people to do things they otherwise were not able to do. The proliferation of computers and telecommunications equipment allows people to share ideas more freely and associate with like-minded people. Sometimes these groups are politically motivated and if they engage in certain political activities, their members are activists. When these politically motivated groups are also hackers and decide to use their computer skills for political reasons, the portmanteau "hacktivists" applies.[100]

In 2011, a group calling itself LulzSec stated that it would conduct fifty days of computer attacks and then disband.[101] Members of LulzSec included members of other groups, including Anonymous and the Internet Feds. Although the group never had a coherent ideology or declared mission statement, its internal communications claimed it attacked websites and organizations that deserved it because of some wrongdoing.[102]

The organizations LulzSec attacked included the internet company America Online, AT&T, the Central Intelligence Agency, the US Senate, an infrastructure security group associated

---

[100] Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (New York: Little, Brown, and Company, 2012), 477-478.

[101] Elizabeth Flock, "LulzSec Disbands: A Timeline of 50 Days of Hacks," *The Washington Post*, June 27, 2011, accessed September 13, 2014, http://www.washingtonpost.com/blogs/blogpost/post/lulzsec-disbands-a-timeline-of-50-days-of-hacks/2011/06/27/AGAmqfnH_blog.html.

[102] Olson, *We Are Anonymous*, 131-132, 244-247, 258-261.

with the Federal Bureau of Investigation, Sony, and the Public Broadcasting Service (PBS). Although the reasons for some of these might be obvious because of the group's anti-authority ideology, some of its victims are not as clear. For example, the defacement of the PBS website was retaliation for a documentary that criticized Wikileaks founder Julian Assange. Part of the defacement denounced the PBS news show Frontline and called for the release of Bradley Manning, the soldier convicted of giving hundreds of thousands of classified files to Wikileaks.[103] The explanation for the group disbanding and stopping its attacks after fifty days was that they were getting bored. [104]

Although LulzSec struck targets it deemed to have a political argument against, it cannot be proved that all of their targets truly warranted attacks based on LulzSec's own logic. Given their tactic for looking through random website for vulnerabilities, it is just as likely that LulzSec members identified some targets based on weaknesses before coming up with justifications for their attack. After all, it is logically inconsistent that an organization that claims to support freedom of speech and the press would attack a media organization simply for publishing a report unsympathetic to a person or cause for whom LulzSec has some affinity. This method of identifying weaknesses before the political justification would make the fifty days of attacks far more certain, especially if there was low-hanging fruit. Some of these targets earned the ire of more ethical hackers who thought LulzSec brought a bad light on the hacking community. This friction would cause problems for the group as other hackers sought to uncover their identities. [105]

Before LulzSec finished its fifty days of attacks, law enforcement authorities began closing in. British law enforcement agency, Scotland Yard, arrested LulzSec member Ryan Cleary

---

[103] Kevin Poulson, "Hacktivists Scorch PBS in Retaliation for WikiLeaks Documentary," *Wired*. May 30, 2011, accessed October 29, 2014, http://www.wired.com/2011/05/lulzsec/.

[104] Flock "LulzSec Disbands: A Timeline of 50 Days of Hack."

[105] Olson, *We Are Anonymous*, 245-247.

on June 21, 2011 because of the group's attack on the Serious Organised [sic] Crime Agency.[106] Four days later, the group announced it was finished.[107] A month later, they arrested the group's spokesman, Jake Davis.[108] Despite immediately denying any connection to Ryan Cleary after his arrest, LulzSec released no information after the arrest of Davis.[109] This silence was a good indicator he was the spokesman since his incarceration would have prevented him posting any information to their Twitter account.[110]

Eventually, law enforcement authorities tracked down and arrested the rest of the group, except for one hacker.[111] The Federal Bureau of Investigation (FBI) had confronted a leader in the group, Hector Xavier Monsegur, with multiple computer crimes, as well as fraud, theft, drugs, and weapons charges and convinced him to work as an informant.[112] The FBI and Scotland Yard arrested the remaining individuals based on information gleaned from Monsegur's cooperation. In the end, courts sentenced LulzsSec members from twenty months to ten years in prison for their

---

[106] David Batty, "Hacking Suspect Ryan Cleary Suffers from Autism, Court Told," *The Guardian*, June 25, 2011, accessed October 30, 2014, http://www.theguardian.com/technology/2011/jun/25/hacker-ryan-cleary-diagnosed-autism.

[107] Flock "LulzSec Disbands: A Timeline of 50 Days of Hack."

[108] British Broadcasting Corporation News, "LulzSec: Shetland Teen Charged Over Computer Hacking Claims," *BBC News UK*, July 31, 2011, accessed October 30, 2014, http://www.bbc.co.uk/news/uk-14359933.

[109] Stephen Chapman, "Suspected LulzSec Player Arrested, In Custody in London," *ZDNet*, June 21, 2011, accessed October 30, 2014, http://www.zdnet.com/blog/security/suspected-lulzsec-player-arrested-in-custody-in-london/8831.

[110] Zack Whittaker, "LulzSec 'Spokesperson' Arrested by Scotland Yard," *ZDNet*, July 27, 2011, accessed September 7, 2014 http://www.zdnet.com/blog/igeneration/lulzsec-spokesperson-arrested-by-scotland-yard/11759.

[111] Olson, *We Are Anonymous*, 406, 458.

[112] Kim Zetter, "Government Seeks Seven-Month Sentence for LulzSec Leader 'Sabu'," *Wired*, May 24, 2014, accessed October 30, 2014, http://www.wired.com/2014/05/sabu-time-served-sentence/.

actions. The court sentenced Monsegur to time served plus a year of supervised release as a reward for his cooperation of the FBI's investigation.[113]

The US government was able to attribute some of the online activities to Monsegur potentially through three different means. The first way was the identification of his computer's Internet Protocol address, a unique identifier that computer networks assign to equipment on that network. Monsegur made a mistake while entering into a chatroom and did not mask this identifier. [114] Hackers who disagreed with Monsegur and LulzSec used this information to track him down, determine his name, and published this information. The second attribution technique was through his mistake in registering a domain name under his real name and mentioning it in online discussions.[115]

The third way the government confirmed his identity was through the FBI. Although the specific details are not public, the FBI visited Monsegur on June 7, 2011 – after his online opponents published his information. Whether the FBI monitored these online exchanges or used their own techniques is not public. However, after confronting him with information, he apparently confirmed his online alias and agreed to cooperate with the investigation. From this meeting on, Monsegur used his relationships with the other members of LulzSec against them to protect himself from a lengthy prison sentence.[116]

---

[113] Ed Pilkington, "LulzSec Hacker 'Sabu' Released After 'Extraordinary' FBI Cooperation," *The Guardian*, May 27, 2014, accessed October 30, 2014, http://www.theguardian.com/technology/2014/may/27/hacker-sabu-walks-free-sentenced-time-served.

[114] Peter Bright, "Doxed: How Sabu Was Outed by Former Anons Long Before His Arrest," *Ars Technica,* March 6, 2012, accessed November 2, 2014, http://arstechnica.com/tech-policy/2012/03/doxed-how-sabu-was-outed-by-former-anons-long-before-his-arrest/.

[115] Olson, *We Are Anonymous*, 209-214.

[116] Chad Bray, "FBI's 'Sabu' Hacker Was a Model Informant," *The Wall Street Journal*, March 9, 2012, accessed November 2, 2014, http://online.wsj.com/articles/SB10001424052970204603004577269844134620160.

During the time of the LulzSec attacks, numerous media reports indicated that computer attacks were rising. While there is no authoritative data available since many attacks are unknown or unreported, there was a prolonged period of hacktivist attacks during this time. Although hacktivism has existed for years, it appeared to increase dramatically around February 2011 and continued through the arrests of the LulzSec members. [117] Suddenly, hackers were suddenly stepping out of the shadows and into the political spotlight to publicize their causes. Anonymous and LulzSec were two of these groups that attacked governments, companies, and other groups with an online presence with impunity, aided by the anonymity of the internet.

However, once a member of LulzSec made a mistake and forgot to mask his identifying information before going online, he lost this anonymity. After this slip up, traditional police work helped to undo the group conspiring to commit computer crimes across the globe. Because the members of these groups lived in the United States, Great Britain, and Ireland, they faced competent modern law enforcement agencies willing to bring them to justice. Frequently taken for granted, a functioning law enforcement and court system gives a country its ability to either deter individuals from engaging in crime or sanctioning them with legal penalties if they are not deterred.

After the LulzSec arrests, hacktivism appeared to cool significantly within the United States. A new group attempted to pick up the LulzSec moniker and hacked a military dating website as a show of support under the name "LulzSec Reborn."[118] After the initial response to the arrests, this group has shown very little activity online and on its Twitter account.[119] The latest

---

[117] Olson, *We Are Anonymous*, 43.

[118] Hayley Tsukayama, "'LulzSec Reborn' claims attack on military dating site," *The Washington Post*, March 28, 2012, accessed September 13, 2014, http://www.washingtonpost.com/business/technology/lulzsec-reborn-claims-attack-on-military-dating-site/2012/03/28/gIQA0UkJgS_story.html.

[119] LulzSec Reborn, "LulzSec Reborn," *Twitter.com*, March 8, 2012, accessed November 16, 2014, https://twitter.com/lulzboatr.

concern does not appear to be highly publicized attacks, like the "fifty days of hacks," but that some states have co-opted hacktivism as another tool in inter-state and intra-state conflicts.[120] Anonymous still mounts an occasional attack, for example against the Ferguson, MO police department in August 2014 after the shooting of Michael Brown, or against the Fort Lauderdale, FL Police Department in December 2014 to protest the city's treatment of the homeless.[121] These are smaller attacks focused on cases of perceived government abuse of power instead of the massive data thefts LulzSec committed. However, hacktivist attacks within the United States appears to have slowed and become smaller in scope since 2012.

The threat of prosecution by the FBI is not exclusive to the United States and Britain. Effective police work can deter hackers from other countries whose governments may cooperate with the US or hackers who may travel to the United States. In 2004 a group of Peruvian hackers, unaffiliated with LulzSec but calling itself LulzSecPeru, stated that they will attack their own government's computers but they will not touch US government systems because of their fears of the FBI.[122]

Effective police work and publicized trials may be the most effective deterrent against non-state hackers. In a recent survey, eighty-six per cent of hackers at a 2014 conference said they

---

[120] Verisign, "Sneak Peek: 2014 iDefense Cyber Threats and Trends Report," *Verisign: Between the Dots*, January 18, 2014, accessed December 4, 2014, http://blogs.verisigninc.com/blog/entry/sneak_peek_2014_idefense_cyber.

[121] William E. Lewis, Jr., "Hacktivist Group Anonymous Crashes Fort Lauderdale Governmental Websites," *Fort Lauderdale City Buzz Examiner*, December 1, 2014, accessed December 4, 2014, http://www.examiner.com/article/hacktivist-group-anonymous-crashes-fort-lauderdale-governmental-websites?cid=PROG-HomepageBlock1-Article-HacktivistGroupAnonymous; David Hunn, "How Computer Hackers Changed the Ferguson Protests," *St. Louis Post Dispatch*, August 13, 2014, accessed December 4, 2014, http://www.stltoday.com/news/local/crime-and-courts/how-computer-hackers-changed-the-ferguson-protests/article_d81a1da4-ae04-5261-9064-e4c255111c94.html.

[122] The Associated Press, "Top South America Hackers Rattle Peru's Cabinet," *The Washington Post*, September 2, 2014, accessed September 13, 2014, http://www.washingtonpost.com/business/technology/top-south-america-hackers-rattle-perus-cabinet/2014/09/02/9d56df0e-3256-11e4-9f4d-24103cb8b742_story.html.

did not think law enforcement would catch them.[123] This perspective would be hard to maintain in the face of rigorous legal action, whether civil or criminal.

Analysis

Event	Political Objective	Attribution	Attacker	Offensive Capability	Political Will
Estonia	Stop removal of Russian statue	Yes	State-backed groups	Unknown – presumed yes	No
Stuxnet	Disrupt Iranian nuclear program	Delayed	National government(s)	No	Yes
LulzSec	Protest perceived government or corporate oppression	Yes	Hacktivist collective	Yes	Yes

Table 1: Comparison of Case Studies

Examining these different cases presents several lessons, not solely restricted to attribution. Although attribution is a necessary component of response, it is not sufficient to trigger a counterattack on its own. In all three cases, the defenders were able to identify the origin of the attacks with different degrees of specificity and timeliness. Only in the LulzSec case did authorities take action stronger than diplomatic protest. In the cases of Estonia and Stuxnet, attribution did not seem to be the obstacle to enacting a deterrent punishment. Estonia appeared to fear an escalation of the conflict with a far more powerful neighbor. Iran did not appear to know an attack was ongoing and later it did not have an offensive cyber capability with which to respond. It is possible, however, that the lack of clear attribution may have inhibited Iran from physically attacking US and Israel for Stuxnet. It only responded with deniable cyber attacks after *The New York Times* attributed the attack. At this point, US officials did not know if these Iranian attacks were a response to Stuxnet or new sanctions.

[123] Dara Kerr, "Vast Majority of Hackers Believe They're Above the Law – Survey," *CNet*, August 14, 2014, accessed November 16, 2014, http://www.cnet.com/news/vast-majority-of-hackers-believe-theyre-above-the-law/.

Just because a defender can attribute an attack, it does not mean that it will retaliate, much less launch a cyber counterattack. In the case of a major power, the attack may not meet response criteria. For a less powerful state, it may fear escalation or transfer of the conflict out of the cyber domain. This unwillingness to respond undermines the credibility of the deterrent threat and probably has a greater effect than the murkiness of attribution in cyberspace.

What this offers is a more nuanced view of attacks in cyberspace. Instead of the alarmist talk of a "cyber Pearl Harbor" or a "cyber Hiroshima," it would be more accurate to discuss lower level attacks that harass or disrupt rather than destroy. After all, the United States does not bomb every country that hassles American tourists or businesses. Even if an attack killed a few Americans, it is unlikely that the US response would be to turn off all of the electricity in the attacking country. As the US Secretary of State stated in response to the 1969 North Korean military downing an American intelligence aircraft, "The weak can be rash. The powerful must be more restrained."[124] Not every provocation deserves a response, especially if the attack can be absorbed or response will betray unknown techniques or technologies. Additionally, the problems of proportionality and discrimination would prevent a widespread US response outside of a declared state of hostilities.

Among the other lessons drawn from these three cases, Martin Libicki's decision loop model for developing options to respond to a cyber attack is a very useful tool. It helps analyze the thought process of the leaders in these events by mapping known information and broad response options. Given the high level of technical expertise in Estonia, it is likely the government had the capability to respond to the Russian cyber attacks but assessed that a

---

[124] Robert Jervis, *System Effects: Complexity in Social and Political Life* (Cambridge: Cambridge University Press, 1997), 255-256, accessed December 1, 2014, http://web.a.ebscohost.com.lumen.cgsccarl.com/ehost/viewarticle?data=dGJyMPPp44rp2%2fdV0%2bnjisfk5Ie46bBRtqm0S6%2bk63nn5Kx95uXxjL6nsEe1pbBIr6qeT7iotFKvpp5oy5zyit%2fk8Xnh6ueH7N%2fiVauqsUmzrbNMr5zqeezdu33snOJ6u%2bnngKTq33%2b7t8w%2b3%2bS7T7Wvskq1qrI%2b5OXwhd%2fqu4ji3MSN6uLSffbq&hid=4204.

counterattack would do more harm than good by losing control of the situation.[125] This resulted in the muted response: Estonia protested through diplomatic channels and tried one of the attackers who lived in Estonia. Any actions stronger than this might have provoked a stronger reaction from Russia and would have been counterproductive.

In Iran, the scientists may have been stuck in the first block of Libicki's model, since some reports show they were unsure of why their uranium enrichment program continually encountered so many problems. After media reports linked Stuxnet to the US and Israeli governments, Iran appears to have chosen to respond with *sub rosa* cyber attacks against US interests and allies. It is also important to recognize what did not happen – Iran did not escalate into physical attacks against, despite a long history of sponsoring terrorism and using proxy groups against its military adversaries. This shows a type of proportionality in responses that some victims will use cyber attacks to respond to the initial cyber attacks because the victim will enjoy a similar level frustrated attribution as the original attack. This proportionality may also prevent escalation to kinetic military strikes.

The United States knew immediately that LulzSec was responsible for its attacks because the group claimed credit for its actions. The attribution problem became identifying the real life identities of the online personas claiming credit for the attacks, not identifying which state or group committed the attack. By confirming that the actions of the group were likely not state-sponsored, it became a matter for law enforcement as indicated on Libicki's model. Unlike in the first two examples, the states involved were able to utilize their judicial systems to prosecute the offenders. This meant that the decision loop ended very quickly after law enforcement authorities identified the actions as criminal in nature as opposed to the actions of another state. Identifying an interstate cyber conflict would have required integrating the response into the national strategy

[125] Libicki, *Cyberdeterrence and Cyberwar*, 99.

vis a vis the attacking state. For LulzSec, coordination between law enforcement authorities helped confirm identities and shut the group down nearly simultaneously.

The third issue these incidents illustrate is that responding to an attack is not as black and white as some authors have made it appear. There are many options on the spectrum of response and these actions are subject to the strength of the attribution, the capabilities of the opponents, their relationship with each other within the strategic context, the will of the attackers and defenders, and alternatives available to them other than cyber attacks.

Contrary to some assertions, attribution does not have to be highly reliable or precise. A state, or its proxies, will likely respond if the attack is serious enough. The state will keep the response further from itself the less certain it is about attribution. If attribution is accurate and precise, then the defender can take official actions as severe against the attacker as it would in other circumstances. At a lower level of attribution, the defending state can take unofficial or undeclared actions, as described by Libicki's *sub rosa* war. If attribution is weaker still, the state can keep the attack at arm's length by using proxies or allowing citizens to attack without fear of legal prosecution.

The capabilities of the opponents are critical to deciding the appropriate response. Just as states must always balance their interests and capabilities in the physical world, the same is obviously true in cyber space. If a state borders Russia, it cannot expect to retaliate to an attack without expecting a threat of escalation. Many experts assume Russia has a robust offensive cyber capability, so this may also act as a deterrent to weaker states trying to level the playing field through cyber attacks. Similarly, if a country mounts a punitive counterattack against infrastructure in the United States resulting in death or destruction of property, the US government could potentially retaliate with a similar strike in cyberspace or even using kinetic military strikes.[126]

[126] Clarke and Knake, *Cyber War*, 177-178.

The relationship between the states involved will also determine available options. The United States will treat attackers located within Great Britain, China, and Russia differently. The very cooperative relationship between the United States and Great Britain will likely result in law enforcement authorities working together to stop an attack, since it is highly unlikely that these governments would attack each other. The extensive cyber espionage committed by China against the United States has resulted in counter-accusations, diplomatic protests, and indictments of five People's Liberation Army officers despite the minimal expectations that these officers would ever stand trial.[127] Russia typically refuses cooperation in most cyber incidents and experts regard criminal attacks against companies in the United States as having the tacit consent of the Russian government.[128] Taken in context of the current poor relations between the Putin administration and the West, there is little expectation that the Russian government would willingly help stop cyber attacks against the United States.

Based on these observations, another proposal is apparent – that offensive capabilities are necessary and useful to respond to attacks. Since cyber attacks require less attribution than kinetic military strikes and the target is usually an adversary already identified to have malignant intentions, offensive cyber capabilities offer the ability to respond in a proportional manner. This allows states to register their complaints more forcefully than a strongly worded letter to another country already suspected of doing harm, without escalation beyond what harm already exists. If other elements of the situation are roughly equal (i.e., the defending state won't provoke or give a disproportionately large and powerful neighbor cause to invade with military forces), then the

---

[127] Federal Bureau of Investigation, "Five Chinese Military Hackers Charged with Cyber Espionage Against U.S.," May 19, 2014, accessed November 30, 2014, http://www.fbi.gov/news/news_blog/five-chinese-military-hackers-charged-with-cyber-espionage-against-u.s; Tom Donilon, "Remarks By Tom Donilon, National Security Advisor to the President: 'The United States and the Asia-Pacific in 2013,'" March 11, 2013, accessed December 2, 2014, http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

[128] "The Russian Business Network: Survey of a Criminal ISP," Verisign, June 27, 2007, accessed December 7, 2014, http://www.verisign.com/static/042674.pdf

defender can theoretically respond in a perfectly symmetrical fashion to an attack. Although perfect symmetry in conflicts is rarely decisive, a proportional and discriminate cyber attack permits the defender to counterattack to either raise the cost of the attack or potentially stop it at its source. This also helps keep the use of coercion within the responsibility of states and governments by giving them the capability and responsibility for protecting their constituents from attacks, through either law enforcement or counterattack. To abdicate this responsibility invites in third parties and may be destabilizing, given the vast amounts of experience available in the private sector.

Counterarguments and Opportunities for Additional Research

No set of case studies is foolproof and it is possible there are problems with those events reviewed herein. To deal with some of the most obvious counterarguments, the following issues will be examined: case study selection, the weakness of capability, the weakness of credibility, and alternatives to cyber attacks.

While it is certainly true the Estonia, Stuxnet, and LulzSec case studies are dissimilar, this does not mean they are not useful for comparison. The differences between these cases allow a broad range of circumstances to be applied against a model, like Martin Libicki's decision loop. To develop a more comprehensive analysis of a particular type of attack or dynamic, it will be necessary to study cases that have more in common with each other, such as the 2007 Estonian attack, the 2008 Georgian attack, and the 2009 attack on Kyrgyzstan.[129] However, the Georgian attack may not yield useful information since it supported kinetic military operations – a significant differentiator from other cyber attacks.

Iran clearly did not have a credible or capable deterrent threat in terms of cyber attacks in 2008, when the first Stuxnet attacks began. It is arguable that Stuxnet provoked Iran into

[129] Christian Czosseck and Kenneth Geers, *The Virtual Battlefield: Perspectives on Cyber Warfare* (Washington, DC: IOS Press, 2009), v.

developing its cyber attack and espionage capabilities, since they did not appear to exist prior to the discovery of Stuxnet. This indicates that Iran believes that a second-strike cyber capability is necessary to preventing cyber attacks and supports the idea of developing an offensive cyber capability to support cyberdeterrence from the Iranian perspective. But given the long history of conflict between Iran versus the United States and Israel, it is also possible that Iran would have developed these capabilities and used them against the United States and Israel regardless of attribution for Stuxnet. Iran's long-time sponsorship of Hezbollah, anti-US insurgents in Iraq, and many other terrorist attacks makes it likely Iranian development of offensive cyber capabilities was a question of "when", not "if."

As Clarke and Knack have already stated, no state has executed a cyber attack on the scale of a nuclear weapon test. There may be a lack of deterrent capability without the demonstration of a Hiroshima attack or Bikini Atoll test since sceptics can dismiss threats as empty bluster. While this skepticism or ignorance may be true for the general population, it is doubtful that countries with advanced cyber programs would allow themselves this luxury. The US government proved the capabilities of physically destructive cyber attacks in its Aurora tests at the Idaho National Labs.[130] It also allegedly performed similar tests on centrifuges identical to the Iranian equipment to ensure that Stuxnet would work prior to executing the attack against Natanz. It is likely that any government investing so much time and money into a critical attack would conduct a rehearsal to ensure the reliability of its tools. Countries with similar offensive capabilities are likely aware of the destructive potential of a well-designed cyber attack. Additionally, while the United States may not know the thought process of other countries' leaders and why they may or may not engage in cyber attacks, President Obama has explained the risks of using cyber as a weapon and cautioned against using it too frequently because of the US

[130] Clarke and Knake, *Cyber War*, 191.

vulnerabilities.[131] This desire to prevent arming one's adversaries or creating a new norm of the acceptability of cyber attacks may act as a restraint, at least for major powers like the United States.

Lastly, the effectiveness of deterring a cyber attack is in question if the alternative is worse than blowback from the cyber attack. In the example of Stuxnet, it is hard to determine if Iran could ever deter the United States and Israel from employing a cyber attack when the alternative is Iran possessing nuclear weapons. In this situation, it is possible that the United States and Israel would still conduct such an attack even if Iran could positively attribute the attack with one hundred per cent certainty. The Iranian response to the cyber attack would still be less dangerous than a nuclear-armed Iran.

Conclusion

Cyberspace is a relatively new and poorly understood domain of human activity. Despite the potential for expression, exchange of knowledge, and creation, it quickly became another area for human conflict. These conflicts range from the petty to major state competition for power and resources. To explore the likelihood of deterrence providing some level of stability and peace, this monograph examined three different cyber attacks, the ability for the victims to attribute the attack, the response chosen, and the effect on future cyber attacks.

Across the three different incidents, there are different dynamics at work. The DDoS attack against Estonia was a low-grade nuisance, whose broad attack base supported plausible deniability by a single actor. The Estonian government suspected Russian government involvement, but could not publicly attribute it to specific actors. Even if they could attribute it, there is the question of whether or not the Russian government would have helped stop the attacks. Given the unwillingness of the Russian government to assist in the investigation and the

[131] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."

repeated statements that the attacks were simply acts of civil disobedience by concerned patriots, it is unlikely the Russian government would have helped stop the attack.

Stuxnet illustrated what happens when top tier cyber powers attack a government. This attack resulted in the destruction of equipment but it is unknown if the Iranian scientists even knew they were the victims of a cyber attack. The malware eventually spilled over onto systems unrelated to Iranian uranium processing and triggered an international effort to determine its origin and nature. Although the authors of the program remain unknown, open source media reports that the US and Israeli governments are responsible. Soon after these revelations, groups linked to Iran attacked Israel, the United States, and its allies with a range of less sophisticated, but high volume attacks. Over time, Iran increased the sophistication of the attacks and began engaging in cyber espionage.

LulzSec was an internationally dispersed hacktivist group who claimed that they hacked computer systems for fun while maintaining the veneer that they chose their targets based on some alleged wrongdoing. They were unaffiliated with any government and generally anti-authority in nature. Since they operated within the United States and countries with effective and cooperative law enforcement agencies, the host nation governments tracked them down and prosecuted the group's members for the laws they violated using computers.

Attribution is critical to defending against and responding to cyber attacks but it is not the only critical component. Cybersecurity professionals, private sector executives, and government leadership need to maintain the ability to identify attacks and the parties responsible to respond appropriately. For cybersecurity specialists, it is a technical matter of stopping attacks. For executives, identifying attackers assists in taking legal actions against the perpetrators when possible and interacting with law enforcement or intelligence agencies. Government leadership must be able to respond to attacks appropriately to protect national interests. Attribution is only one component of an entire system but without it, any response is doomed to failure.

Bibliography

Agence France-Presse. "U.S. says Iran behind cyber attack in Saudi Arabia." *Al Arabiya News.* October 13, 2012. Accessed October 26, 2014. http://english.alarabiya.net/articles/2012/10/13/243475.html.

Arnold, Chloe. "Russian Group's Claims Reopen Debate On Estonian Cyberattacks." *Radio Free Europe / Radio Liberty.* March 30, 2009. Accessed September 30, 2014. http://www.rferl.org/content/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html.

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" November 1993. Accessed November 11, 2014). http://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf.

The Associated Press. "Top South America Hackers Rattle Peru's Cabinet." *The Washington Post.* September 2, 2014. Accessed September 13, 2014. http://www.washingtonpost.com/business/technology/top-south-america-hackers-rattle-perus-cabinet/2014/09/02/9d56df0e-3256-11e4-9f4d-24103cb8b742_story.html.

Barnes, Julian E., and Siobhan Gorman. "U.S. Says Iran Hacked Navy Computers." *The Wall Street Journal.* September 27, 2013. Accessed October 26, 2014. http://online.wsj.com/articles/SB10001424052702304526204579101602356751772.

Batty, David. "Hacking Suspect Ryan Cleary Suffers from Autism, Court Told." *The Guardian.* June 25, 2011. Accessed October 30, 2014. http://www.theguardian.com/technology/2011/jun/25/hacker-ryan-cleary-diagnosed-autism.

Bray, Chad. "FBI's 'Sabu' Hacker Was a Model Informant." *The Wall Street Journal.* March 9, 2012. Accessed November 2, 2014. http://online.wsj.com/articles/SB10001424052970204603004577269844134620160.

Bright, Peter. "Doxed: How Sabu Was Outed by Former Anons Long Before His Arrest." *Ars Technica.* March 6, 2012. Accessed November 2, 2014. http://arstechnica.com/tech-policy/2012/03/doxed-how-sabu-was-outed-by-former-anons-long-before-his-arrest/.

British Broadcasting Corporation News. "LulzSec: Shetland Teen Charged Over Computer Hacking Claims." *BBC News UK.* July 31, 2011. Accessed October 30, 2014. http://www.bbc.co.uk/news/uk-14359933.

Bruno, Greg. "State Sponsors: Iran." *The Council on Foreign Relations.* October 13, 2011. Accessed November 20, 2014. http://www.cfr.org/iran/state-sponsors-iran/p9362.

Carnegie Mellon University CERT. *About Us.* 2014. Accessed October 2, 2014). http://www.cert.org/about/.

Chapman, Stephen. "Suspected LulzSec Player Arrested, In Custody in London." *ZDNet.* June 21, 2011. Accessed October 30, 2014. http://www.zdnet.com/blog/security/suspected-lulzsec-player-arrested-in-custody-in-london/8831.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: HarperCollins Publishers, 2010.

Clayton, Mark. "Cyber-war: In Deed and Desire, Iran Emerging as a Major Power." *The Christian Science Monitor.* March 16, 2014. Accessed October 26, 2014. http://www.csmonitor.com/World/ Security-Watch/Cyber-Conflict-Monitor/2014/0316/Cyber-war-In-deed-and-desire-Iran-emerging-as-a-major-power.

Cylance. "Operation Cleaver." *Cylance.* December 1, 2014. Accessed December 4, 2014. http://www0.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf.

Czosseck, Christian, Kenneth Geers. *The Virtual Battlefield: Perspectives on Cyber Warfare.* Washington, DC: IOS Press, 2009.

Danchev, Dancho. *Coordinated Russia vs Georgia cyber attack in progress.* August 11, 2008. Accessed October 5, 2014. http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670.

Donilon, Tom. *Remarks By Tom Donilon, National Security Advisor to the President: The United States and the Asia-Pacific in 2013."*March 11, 2013. Accessed December 2, 2014. http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a

Echevarria, Antulio J. II. "Fourth-Generation War and Other Myths." *Strategic Studies Institute.* November 2005. Accessed November 13, 2014. http://www.strategicstudiesinstitute.army.mil/ pdffiles/pub632.pdf.

The Economist. "A Cyber-Riot." *The Economist.* May 27, 2007. Accessed September 1, 2014. http://www.economist.com/node/9163598.

Federal Bureau of Investigation. *Five Chinese Military Hackers Charged with Cyber Espionage Against U.S.* May 19, 2014. Accessed November 30, 2014. http://www.fbi.gov/news/news_blog/five-chinese-military-hackers-charged-with-cyber-espionage-against-u.s.

Feith, David. "Timothy Thomas: Why China Is Reading Your Email; Beijing's cyber attacks are rooted in military strategy, says one of America's foremost experts. The best way to combat them is for the U.S. to go on the cyber offensive too." *ProQuest.* March 29, 2013. Accessed December 2, 2014. http://search.proquest.com.lumen.cgsccarl.com/docview/1321561425?pq-origsite=summon.

Flock, Elizabeth. "LulzSec Disbands: A Timeline of 50 Days of Hacks." *The Washington Post.* June 27, 2011. Accessed September 13, 2014. http://www.washingtonpost.com/blogs/blogpost/post/lulzsec-disbands-a-timeline-of-50-days-of-hacks/2011/06/27/AGAmqfnH_blog.html.

Freedman, Lawrence. *Deterrence.* Malden, MA: Polity Press, 2004.

—. *Strategy: A History.* New York: Oxford University Press, 2013.

Gat, Azar. *A History of Military Thought* . New York: Oxford University Press, 2001.

Gobry, Pascal-Emmanuel. "The Internet Is 20% Of Economic Growth." *Business Insider.* May 24, 2011. Accessed October 2, 2014. http://www.businessinsider.com/mckinsey-report-internet-economy-2011-5?op=1.

Goodwins, Rupert. "Stuxnet has put us all on the front line of warfare 2.0." *ZDNet.* June 1, 2012. Accessed October 8, 2014. http://www.zdnet.com/stuxnet-has-put-us-all-on-the-front-line-of-warfare-2-0-3040155333/.

Goure, Daniel. “Prepare for Cyber Armageddon.” *The Lexington Institute*. December 9, 2014. Accessed December 15, 2014. http://www.lexingtoninstitute.org/prepare-for-cyber-armageddon/.

Gray, Colin. *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling.* Carlisle, PA: US Army War College Press, 2013.

Gross, Michael J. "A Declaration of Cyber-War." *Vanity Fair.* April 2013. Accessed December 4, 2014. http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

Hildreth, Steven A. "Cyberwarfare." In *Cyberwarfare: Terror at a Click* , by John V., ed. Blane, 1-22. Huntington, NY: Novinka Books, 2001.

Hunn, David. "How Computer Hackers Changed the Ferguson Protests." *St. Louis Post Dispatch.* August 13, 2014. Accessed December 4, 2014. http://www.stltoday.com/news/local/crime-and-courts/how-computer-hackers-changed-the-ferguson-protests/article_d81a1da4-ae04-5261-9064-e4c255111c94.html.

Jervis, Robert. *System Effects: Complexity in Social and Political Life.* Cambridge: Cambridge University Press, 1997. Accessed December 1, 2014. http://web.a.ebscohost.com.lumen.cgsccarl.com/ehost/viewarticle?data=dGJyMPPp44rp2%2fdV0%2bnjisfk5Ie46bBRtqm0S6%2bk63nn5Kx95uXxjL6nsEe1pbBIr6qeT7iotFKvpp5oy5zyit%2fk8Xnh6ueH7N%2fiVauqsUmzrbNMr5zqeezdu33snOJ6u%2bnngKTq33%2b7t8w%2b3%2bS7T7Wvskq1qrI%2b5OXwhd%2fqu4ji3MSN6uLSffbq&hid=4204

Kampmark, Binoy. "Cyber Warfare Between Estonia and Russia." *Contemporary Review*, Autumn 2007: 288-293. Accessed December 7, 2014, http://search.proquest.com.lumen.cgsccarl.com/docview/204958799/fulltextPDF?accountid=28992.

Kerr, Dara. "Vast Majority of Hackers Believe They're Above the Law - Survey." *CNet.* August 14, 2014. Accessed November 16, 2014. http://www.cnet.com/news/vast-majority-of-hackers-believe-theyre-above-the-law/.

Kesan, Jay A., and Carol M. Hayes. "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace." *Social Science Research Network.* April 7, 2011. Accessed November 15, 2014. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1805163.

Lachow, Irving. "The Stuxnet Enigma: Implications for the Future of Cybersecurity." *Georgetown Journal of International Affairs*, Fall 2011: 118-126.

Leder, Felix, Tillmann Werner, and Peter Martini. "Proactive Botnet Countermeasures: An Offensive Approach." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, by Christian Czosseck, Kenneth Geers, & eds., 211-225. Washington, DC: IOS Press, 2009.

Lewis, William E. Jr. "Hacktivist Group Anonymous Crashes Fort Lauderdale Governmental Websites." *Fort Lauderdale City Buzz Examiner.* December 1, 2014. Accessed December 4, 2014. http://www.examiner.com/article/hacktivist-group-anonymous-crashes-fort-lauderdale-governmental-websites?cid=PROG-HomepageBlock1-Article-HacktivistGroupAnonymous

Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: Rand Project Air Force, 2009. Accessed December 7, 2014, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

—. "Sub Rosa Cyber War." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck, Kenneth Geers, 53-65. Washington, DC: IOS Press, 2009.

Lind, William S., Keith Nightengale, John F. Schmitt, Joseph W. Sutton, and Gary I. Wilson. "The Changing Face of War: Into the Fourth Generation." *Marine Corps Gazette 85, no. 11 (11, 2001): 65-8,.* November 2001. Accessed November 13, 2014. https://lumen.cgsccarl.com/login?url=http://search.proquest.com.lumen.cgsccarl.com/docview/221496693?accountid=28992.

Lipin, Michael. "Saudi Cyber Attack Seen as Work of Amateur Hackers Backed by Iran." *Voice of America.* October 25, 2012. Accessed October 26, 2014. http://www.voanews.com/content/saudi-arabia-iran-cyber-attack/1533694.html.

Lobel, Hannah. "Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict." *Texas International Law Journal*, Summer 2012: 617-640. Accessed December 7, 2014, http://search.proquest.com.lumen.cgsccarl.com/docview/1018566780?pq-origsite=summon.

LulzSec Reborn. "LulzSec Reborn." *Twitter.com.* March 8, 2012. Accessed November 16, 2014. https://twitter.com/lulzboatr.

Mendes, Sam, dir. *Skyfall*. Twentieth Century Fox, 2012. DVD. Twentieth Century Fox, 2013.

Menn, Joseph. *U.S. cyberwar strategy stokes fear of blowback.* May 10, 2013. Accessed October 8, 2014. http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510.

Moran, Daniel. "Geography and Strategy." In *Strategy in the Contemporary World*. edited by John Baylis, James J. Wirtz, Colin S. Gray, 115-131. Oxford: Oxford Univesity Press, 2013.

Nakashima, Ellen. "Iran Blamed for Cyber Attacks on U.S. Banks and Companies." *The Washington Post.* September 21, 2012. Accessed September 7, 2014. http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html.

Nazario, Jose. "Politically Motivated Denial of Service Attacks." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck, Kenneth Geers, 163-181. Washington, DC: IOS Press, 2009.

The Nuclear Threat Initiative. *Israel | Country Profile | Nuclear.* May 2014. Accessed October 25, 2014. http://www.nti.org/country-profiles/israel/nuclear/.

O Murchu, Liam. "A Malware Anniversary to Remember." *Symantec: Security Response.* July 11, 2011. Accessed November 30, 2014. http://www.symantec.com/connect/blogs/malware-anniversary-remember.

Olson, Parmy. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency.* New York: Little, Brown, and Company, 2012.

Panetta, Leon E. "Remarks by Secretary Panetta to Service Members at US Strategic Command." *U.S. Department of Defense.* August 5, 2011. Accessed November 13, 2014. http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4861.

Paul, T. V. "Complex Deterrence: An Introduction." In *Complex Deterrence: Strategy in the Global Age*, edited by T. V. Paul, Patrick M. Morgan, and James J. Wirtz, 1-27. Chicago, IL: The University of Chicago Press, 2009.

Pellerin, Cheryl. *Rogers: Cybercom Defending Networks, Nation.* August 18, 2014. Accessed October 2, 2014. http://www.defense.gov/news/newsarticle.aspx?id=122949.

Pilkington, Ed. "LulzSec Hacker 'Sabu' Released After 'Extraordinary' FBI Cooperation." *The Guardian.* May 27, 2014. Accessed October 30, 2014. http://www.theguardian.com/technology/2014/may/27/hacker-sabu-walks-free-sentenced-time-served.

Poulson, Kevin. "Hacktivists Scorch PBS in Retaliation for WikiLeaks Documentary." *Wired.* May 30, 2011. Accessed October 29, 2014. http://www.wired.com/2011/05/lulzsec/.

Qiao, Liang, and Xiangsui Wang. *Unrestricted Warfare: China's Master Plan to Destroy America.* Panama City, Panama: Pan American Publishing Company, 2002.

Rid, Thomas. "Think Again: Cyberwar." *Foreign Policy.* February 27, 2012. Accessed November 13, 2014. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar.

Riley, Michael, and Jordan Robertson. "Iran-Backed Hackers Target Airports, Carriers: Report." *Bloomberg.* December 2, 2014. Accessed December 4, 2014. http://www.bloomberg.com/news/2014-12-02/iran-backed-hackers-target-airports-carriers-report.html.

Ruus, Kertu. "Cyber War I: Estonia Attacked from Russia." *The European Institute.* December 02, 2007. Accessed September 1, 2014. http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html.

—. "E-Stonia: Pioneer of Internet Innovation and e-Goverment." *The European Institute.* March 2, 2007. Accessed September 1, 2014. http://www.europeaninstitute.org/20070302100/Spring-2007/estonia-pioneer-of-internet-innovation-and-e-goverment.html.

Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *The New York Times.* June 1, 2012. Accessed October 8, 2014. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

Schaub, Gary Jr. ""When Is Deterrence Necessary? Gauging Adversary Intent"." Winter 2009. Accessed December 7, 2014. http://search.proquest.com.lumen.cgsccarl.com/docview/1429444718?pq-origsite=summon.

Selyukh, Alina, and Patricia Zengerle. *Senate Intelligence Committee Approves Cybersecurity Bill.* July 8, 2014. Accessed October 2, 2014. http://www.reuters.com/article/2014/07/08/us-usa-cybersecurity-congress-idUSKBN0FD2LG20140708.

Shachtman, Noah. *Kremlin Kids: We Launched the Estonian Cyber War.* March 11, 2011. Accessed September 30, 2014. http://www.wired.com/2009/03/pro-kremlin-gro/.

—. *Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It.* March 11, 2009. Accessed October 5, 2014. http://www.wired.com/2009/03/georgia-blames/.

Sharma, Amit. "Cyber Wars: A Paradigm Shift from Means to Ends." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck, Kenneth Geers, 3-17. Washington, DC: lOS Press, 2009.

Sheehan, Michael. "The Evolution of Modern Warfare." In *Strategy in the Contemporary World*, edited by John Baylis, James J. Wirtz, Colin S. Gray, 39-59. Oxford: Oxford University Press, 2013.

Sheldon, John B. "The Rise of Cyberpower." In *Strategy in the Contemporary World*, edited by John Baylis, James J. Wirtz, Colin S. Gray, 303-319. Oxford: Oxford University Press, 2013.

Simons, Anna, Joe McGraw, and Duane Lauchengco. *TheSovereignty Solution: A Commonsense Approach to Global Security.* Annapolis, MD: Naval Institute Press, 2011.

Starr, Stuart H. "Towards an Evolving Theory of Cyberpower." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck, Kenneth Geers, 18-52. Washington, DC: IOS Press, 2009.

Stoll, Clifford. "Stalking the Wily Hacker." *Communication of the ACM*, May 1988: 484-500. Accessed October 2, 2014, http://pdf.textfiles.com/academics/wilyhacker.pdf.

Symantec. *Duqu: The Precursor to the Next Stuxnet.* Accessed November 30, 2014. http://www.symantec.com/outbreak/?id=stuxnet.

Thomas, Timothy. "Russian Views on Information-based Warfare." *Foreign Military Studies Office*. July 1996. Accessed December 2, 2014. http://fmso.leavenworth.army.mil/documents/rusvuiw.htm.

Tsukayama, Hayley. "'LulzSec Reborn' claims attack on military dating site." *The Washington Post.* March 28, 2012. Accessed September 13, 2014. http://www.washingtonpost.com/business/technology/lulzsec-reborn-claims-attack-on-military-dating-site/2012/03/28/gIQA0UkJgS_story.html.

United States Army. *U.S. Army Cyber Command.* Accessed October 2, 2014. http://www.arcyber.army.mil/history_arcyber.html

US Cyber Command Public Affairs. *U.S. Cyber Command*. August 2013. Accessed October 02, 2014. http://www.stratcom.mil/factsheets/2/Cyber_Command/.

US Department of Defense. *Deputy Assistant Secretary of Defense for Cyber Policy.* Accessed October 2 2014, 2014. http://policy.defense.gov/OUSDPOffices/ASDforHomelandDefenseGlobalSecurity/CyberPolicy.aspx.

Van Evra, Stephen .*Guide to Methods for Students of Political Science.* Ithaca, NY: Cornell University Press, 1997.

Verisign. "Sneak Peek: 2014 iDefense Cyber Threats and Trends Report." *Verisign: Between the Dots*. Januray 18, 2014. Accessed December 4, 2014. http://blogs.verisigninc.com/blog/entry/sneak_peek_2014_idefense_cyber.

—. "The Russian Business Network: Survey of a Criminal ISP." June 27, 2007. Accessed December 7, 2014. http://www.verisign.com/static/042674.pdf

The White House. "Remarks by the President on Securing Our Nation's Cyber Infrastructure." May 29, 2009. Accessed September 25, 2014. http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

—. "Cybersecurity." Accessed December 7, 2014. http://www.whitehouse.gov/issues/foreign-policy/cybersecurity

Whittaker, Zack. "LulzSec 'Spokesperson' Arrested by Scotland Yard." *ZDNet.* Jul 27, 2011. Accessed September 7, 2014. http://www.zdnet.com/blog/igeneration/lulzsec-spokesperson-arrested-by-scotland-yard/11759.

Wolff, Josephine. "Howard Schmidt: Hackers and spies have launched attacks on vital computer systems in recent months. White House cyber-security coordinator Howard Schmidt on what it all means." *Newsweek.* January 3, 2011. Accessed December 7, 2014. http://search.proquest.com.lumen.cgsccarl.com/docview/822401947?pq-origsite=summon.

Zetter, Kim. "Government Seeks Seven-Month Sentence for LulzSec Leader 'Sabu'." *Wired.* May 24, 2014. Accessed October 30, 2014. http://www.wired.com/2014/05/sabu-time-served-sentence/.

—. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired.* July 11, 2011. Accessed October 8, 2014. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/.

—. "Legal Experts: Stuxnet Attack on Iran Was Illegal ‘Act of Force’." *Wired.* March 25, 2013. Accessed November 30, 2014. http://www.wired.com/2013/03/stuxnet-act-of-force/.

—. "Sony Hackers Threaten to Release a Huge ‘Christmas Gift’ of Secrets.'" Wired. December 15, 2014. Accessed February 3, 2015. http://www.wired.com/2014/12/sony-hack-part-deux/.